НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет (ННІ) ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету (Директор ННІ)	**Завідувач кафедри**
Інформаційних технологій (назва факультету(ННІ))	Комп'ютерних систем, мереж та кібербезпеки (назва кафедри)
_____ Болбот І.М., д.т.н, проф. (підпис) (ПІБ, вчене звання і ступінь)	_____ Касаткін Д.Ю., к. пед.н., доц. (підпис) (ПІБ, вчене звання і ступінь)
«___»_____2025 р.	«___»_____2025 р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Дослідження та вдосконалення системи керування наземними роботизованими платформами»

Спеціальність 123 «Комп'ютерна інженерія»
(код і найменування)

Освітня програма Комп'ютерні системи та мережі
(назва)

Орієнтація освітньої програми Освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Гарант освітньої програми

д.т.н., доцент	_____	Шкарупило В.В.
(науковий ступінь та вчене звання)	(підпис)	(ПІБ)

Керівник магістерської кваліфікаційної роботи

д.т.н., проф.	_____	Болбот І. М.
(науковий ступінь та вчене звання)	(підпис)	(ПІБ)

Виконав _____ Муха В. В.
(підпис) (ПІБ)

КИЇВ-2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет (ННІ) ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки
к.пед.н., доц. _____ Касаткін Д.Ю.
(вчене звання і ступінь) (підпис) (ПІБ)
«__» _____ 20__ р.

З А В Д А Н Н Я

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧУ

Мусі Віталію Віталійовичу
(прізвище, ім'я, по батькові)

Спеціальність 123 «Комп'ютерна інженерія»
(код і найменування)

Освітня програма Комп'ютерні системи та мережі
(назва)

Орієнтація освітньої програми Освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Тема магістерської кваліфікаційної роботи: «Дослідження та вдосконалення системи керування наземними роботизованими платформами»

затверджена наказом ректора НУБіП України від "29" жовтня 2024р. № 1941 «С»

Термін подання завершеної роботи на кафедру 14 листопада 2025 р.

Вихідні дані до магістерської кваліфікаційної роботи

Перелік питань, що підлягають дослідженню:
1.
2.
3.

Перелік графічного матеріалу (за потреби)

Дата видачі завдання " 29 **"** жовтня 2024 р.

Керівник магістерської кваліфікаційної роботи _____ Болбот І. М.
(підпис) (прізвище та ініціали)

Завдання прийняв до виконання _____ Муха В. В.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 60 сторінок, 14 малюнків, 5 таблиць, 15 джерел.

Об’єкт розробки – Система дистанційного керування наземною роботизованою платформою (НРП) через глобальну мережу 4G/LTE.

Мета роботи – Дослідження та реалізація архітектури керування, що долає обмеження дальності (BVLOS) та вирішує мережеву проблему CG-NAT (Carrier-Grade NAT).

Проект складається з п’яти розділів.

У першому розділі проведено аналіз існуючих P2P (LoRa) та IP (4G/LTE) систем керування.

У другому розділі досліджено програмний стек, обґрунтовано вибір архітектури "клієнт-сервер" та інструментів.

У третьому розділі описано практичну реалізацію: розгортання сервера на AWS EC2 зі статичною Elastic IP та налаштуванням Security Groups ; конфігурацію Raspberry Pi; та автоматизацію всіх процесів за допомогою сервісів systemd .

У четвертому розділі представлено результати тестування. Лабораторні тести підтвердили працездатність програмного стеку "від кінця до кінця" .

У п’ятому розділі обговорено результати, підтверджено придатність системи для повільних НРП . Визначено критичні вразливості (ризик перехоплення) та запропоновано шляхи вдосконалення.

Результатом виконання роботи є розроблений та протестований програмно-апаратний комплекс для глобального керування НРП.

ABSTRACT

Explanatory note: 60 pages, 14 figures, 5 tables, 15 sources.

Object of Development – A remote control system for an unmanned ground vehicle (UGV) via the global 4G/LTE network.

Objective of the work – The research and implementation of a control architecture that overcomes range limitations (BVLOS) and solves the network problem of CG-NAT (Carrier-Grade NAT) .

The first chapter analyzes existing P2P (LoRa) and IP (4G/LTE) control systems.

The second chapter investigates the software stack, justifying the choice of a "client-server" architecture and tools.

The third chapter describes the practical implementation: deploying the server on AWS EC2 with a static Elastic IP and configuring Security Groups ; configuring the Raspberry Pi; and automating all processes systemd services .

The fourth chapter presents the testing results. Lab tests confirmed the end-to-end functionality of the software stack .

The fifth chapter discusses the results, confirming the system's suitability for slow-moving UGVs . Critical vulnerabilities (risk of hijacking) were identified , and improvement paths were proposed.

The result of this work is a developed and tested software-hardware complex for global UGV control.

Зміст

ВСТУП

Розвиток робототехніки у XXI столітті набуває стрімких обертів, а інтеграція автономних і напівавтономних систем охоплює дедалі ширший спектр діяльності людини. Серед цих технологій важливу роль відіграють наземні роботизовані платформи (НРП), або ж безпілотні наземні транспортні засоби (UGV). Вони вже зараз займають значне місце у військово-промисловій сфері, логістиці, моніторингу, сільському господарстві, пошуково-рятувальних операціях та роботах у небезпечному для людини середовищі. Можливість виконання завдань дистанційно, без ризику для здоров'я і життя оператора, підкреслює високу суспільну та економічну важливість розвитку цих технологій.

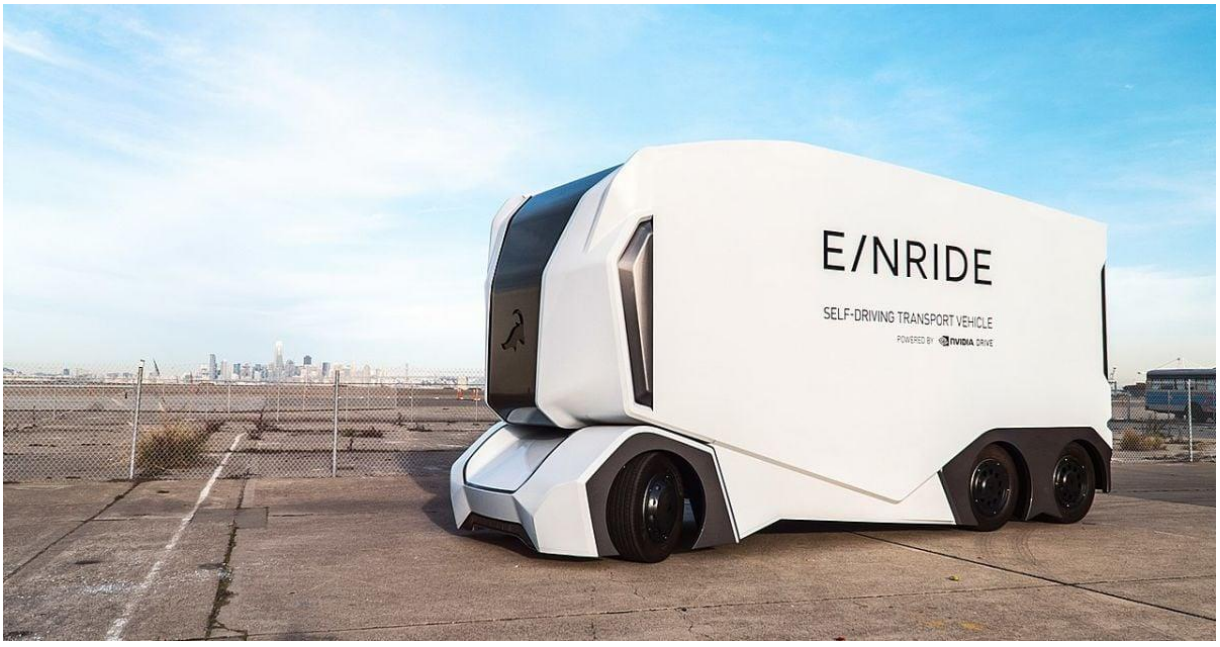

Рисунок 1.1 - Безпілотна вантажівка T-pod

Ефективність роботи наземних роботизованих платформ залежить не лише від якості їхньої механічної частини (шасі, маніпуляторів, силових установок), але й від надійності і функціональності системи керування. У багатьох сучасних випадках робоче середовище є неструктурованим, а зміни умов відбуваються дуже динамічно, тому повна автономність ще не може стати достатньою. Тому телеопераційне керування (teleoperation) залишається

ключовим режимом роботи таких платформ. Цей підхід потребує стабільного та високоефективного каналу зв’язку між оператором і платформою.

Основними завданнями цього каналу є: передача команд керування (C&C) від оператора до платформи, отримання телеметричних даних (дані навігації та стан систем), а також трансляція в реальному часі відеопотоку з бортових камер. Саме відеопотік забезпечує оператору необхідний рівень ситуаційної обізнаності для прийняття ефективних рішень. Відтак система керування повинна відповідати низці суворих вимог: мати мінімальні затримки (low latency), гарантувати високу надійність і стійкість каналу зв’язку, забезпечувати достатню пропускну здатність для передачі відео високої чіткості та працювати на значній відстані. Традиційні системи керування, які використовують виділені радіоканали (Point-to-Point RF), раніше демонстрували низькі показники затримки. Аналогові системи передачі відео дозволяли отримати майже миттєвий зворотний зв’язок. Проте вони мають суттєві обмеження. Перша проблема – обмежена дальність дії, яка залежить від радіогоризонту та прямих умов видимості (Line-of-Sight, LOS). Друга – можливість передачі лише відео низької чіткості (SD), що недостатньо для багатьох сучасних задач ідентифікації й навігації. Третя – вразливість цих каналів до перехоплення й радіоелектронних перешкод.

Ці обмеження сприяли активному пошуку нових архітектурних підходів. Найбільш перспективним напрямом у цьому контексті стало впровадження глобальних комерційних мереж, зокрема технології 4G/LTE, в якості транспортного середовища. Такий підхід дозволяє вирішити одразу дві ключові проблеми: реалізувати потенційно необмежену за відстанню передачу даних (Beyond-Line-of-Sight, BLOS) та забезпечити достатню пропускну здатність для трансляції відео високої роздільної здатності (HD/4K). Це відкриває нові можливості для використання наземних роботизованих платформ у складних умовах міського середовища або на широко розподілених територіях. Однак впровадження інфраструктури 4G/LTE не обмежується

простою заміною каналу зв’язку. Воно породжує цілу низку нових науково-технічних викликів. Зокрема, на відміну від спеціалізованих P2P-каналів, комерційні публічні мережі не забезпечують гарантованої якості обслуговування (Quality of Service, QoS). Використання таких мереж призводить до появи значних, а головне – нерівномірних затримок (jitter) у передачі даних. Ці затримки включають час кодування відео, затримки в ядрах операторських мереж та час декодування, що сумарно може досягати сотень мілісекунд. Подібні особливості унеможливлюють оперативне управління платформою в режимі реального часу. Додатково слід врахувати суттєву залежність від стабільності роботи та територіального покриття зовнішньої інфраструктури. Таким чином, виникає важливе науково-технічне протиріччя між вимогами до функціональності системи (глобальна дальність дії, висока роздільна здатність відео) і необхідними показниками продуктивності (мінімальні затримки, стабільність), що характерно для класичних підходів. Зазначене протиріччя формує наукову актуальність даного дослідження та підкреслює доцільність розробки методів вдосконалення систем управління на основі технології 4G/LTE, спрямованих на мінімізацію їхніх структурних недоліків. Метою даної дипломної роботи є аналіз існуючих систем управління наземними роботизованими платформами та розробка оптимізованої системи управління, що базується на технології 4G/LTE. Зокрема, дослідження спрямоване на вдосконалення програмно-апаратних рішень для зменшення затримок передачі даних і поліпшення стабільності функціонування системи.

Дослідження присвячене процесу телеопераційного управління наземними роботизованими платформами. Головним предметом виступають методики, протоколи та програмно-архітектурні підходи, спрямовані на створення та вдосконалення систем управління НРП із використанням глобальних мереж 4G/LTE. У ході дослідження застосовано комплексний набір методик. Зокрема, теоретичний аналіз науково-технічної літератури для класифікації систем і протоколів; порівняльний аналіз для визначення оптимальних рішень; методи системного проєктування та програмування для розробки прототипу;

експериментальні дослідження для оцінки характеристик системи та статистичні методи для обробки отриманих даних. Структура роботи охоплює вступ, п’ять змістових розділів, висновки та список використаних джерел.

РОЗДІЛ 1. ДОСЛІДЖЕННЯ ІСНУЮЧИХ СИСТЕМ

1.1 Класифікація та огляд архітектур керування наземними роботизованими платформами

Функціонування будь-якої наземної роботизованої платформи нерозривно пов'язане із системою управління, яка забезпечує взаємодію між оператором і машиною. Ця система являє собою поєднання апаратних та програмних компонентів, що реалізують три основні функції: передача команд управління (Command and Control, C&C), отримання телеметричних даних про стан платформи, її навігацію та діагностику, а також передачу відеопотоку в реальному часі, що широко застосовується в сучасних рішеннях. Вибір базової архітектури зв'язку відіграє ключову роль, адже саме він визначає основні експлуатаційні характеристики платформи, такі як дальність роботи, затримку передачі сигналу, пропускну здатність каналу та загальну надійність системи.

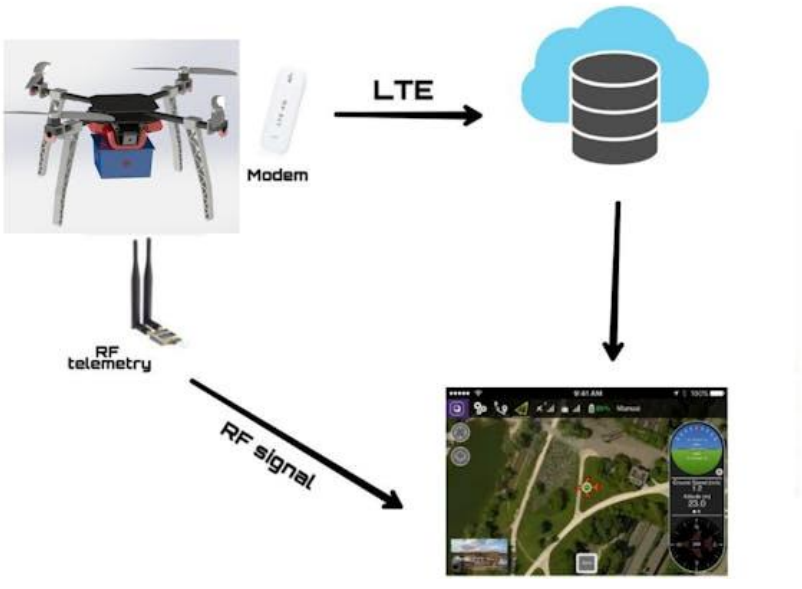

Рисунок 1.2 – Приклад гібридної системи керування безпілотником

Будь-яка архітектура повинна справлятися зі завданням передачі двох принципово різних типів даних. З одного боку, це команди управління — маленькі за обсягом пакети, для яких критично важлива максимально висока надійність і мінімальні затримки. З іншого боку, це відеопотік — значні обсяги даних, що потребують високої пропускної здатності, хоча допускають трохи більші затримки. Саме спосіб розв'язання цього "конфлікту" пріоритетів визначає класифікацію таких архітектур.

Незалежно від обраної архітектури, для забезпечення ефективного та безпечного дистанційного керування будь-яка система має відповідати набору ключових вимог. Передусім важливим є забезпечення низької затримки, адже саме вона визначає швидкість реакції платформи на дії оператора. Не менш суттєвими є надійність і стійкість каналу зв'язку, які гарантують безперервність роботи навіть за умов перешкод або слабкого сигналу. Пропускна здатність каналу також повинна бути достатньою для передачі не тільки команд, а й потоку високоякісних відеоданих. Окрім того, дальність дії системи повинна відповідати завданням, для яких розроблено платформу. Водночас, у контексті передачі інформації, особливо через публічні мережі, визначальною є безпека, яка забезпечує захист каналу управління від стороннього втручання чи несанкціонованого доступу.

Системи керування роботизованими платформами (НРП) можна класифікувати на два основні типи, залежно від способу організації каналу зв’язку. Перший тип включає архітектури з використанням виділених радіоканалів (Point-to-Point, P2P). У цьому разі між станцією оператора і роботизованою платформою встановлюється прямий, безпосередній радіозв’язок. Такий підхід є традиційним і забезпечує незалежність від сторонньої інфраструктури, що гарантує прогнозовану роботу системи та низьку затримку сигналу. Основним обмеженням є залежність від прямої видимості (Line-of-Sight, LOS) або радіогоризонту через фізичні властивості радіохвиль. Щоб відповідати різним вимогам до передачі даних, часто

використовуються гібридні системи: вузькосмуговий радіопротокол для команд управління, стійкий до перешкод і здатний працювати на великій відстані, а також широкосмуговий канал для високоякісного відео, який має меншу дальність дії або проникну здатність. Другий тип — архітектури, засновані на використанні існуючої інфраструктури (Infrastructure-Based). Цей підхід базується на масштабних комунікаційних мережах, зазвичай на комерційних мережах мобільного зв'язку (наприклад, 4G/LTE чи 5G). У такій моделі прямий радіозв'язок між оператором і НРП відсутній; натомість обидва користуються глобальною мережею як клієнти. Основна перевага такого підходу — практично необмежена дальність дії в межах зони покриття мережі, що дозволяє управління навіть за межами прямої видимості (Beyond-Line-of-Sight, BLOS). Крім того, тут зазвичай уніфікуються всі потоки даних—зокрема керування, телеметрія та відео високої чіткості—в єдиний IP-потік. Однак цей підхід також має недоліки: залежність від сторонньої інфраструктури, можливі коливання затримки сигналу (jitter) і ризики щодо безпеки даних у публічних мережах.

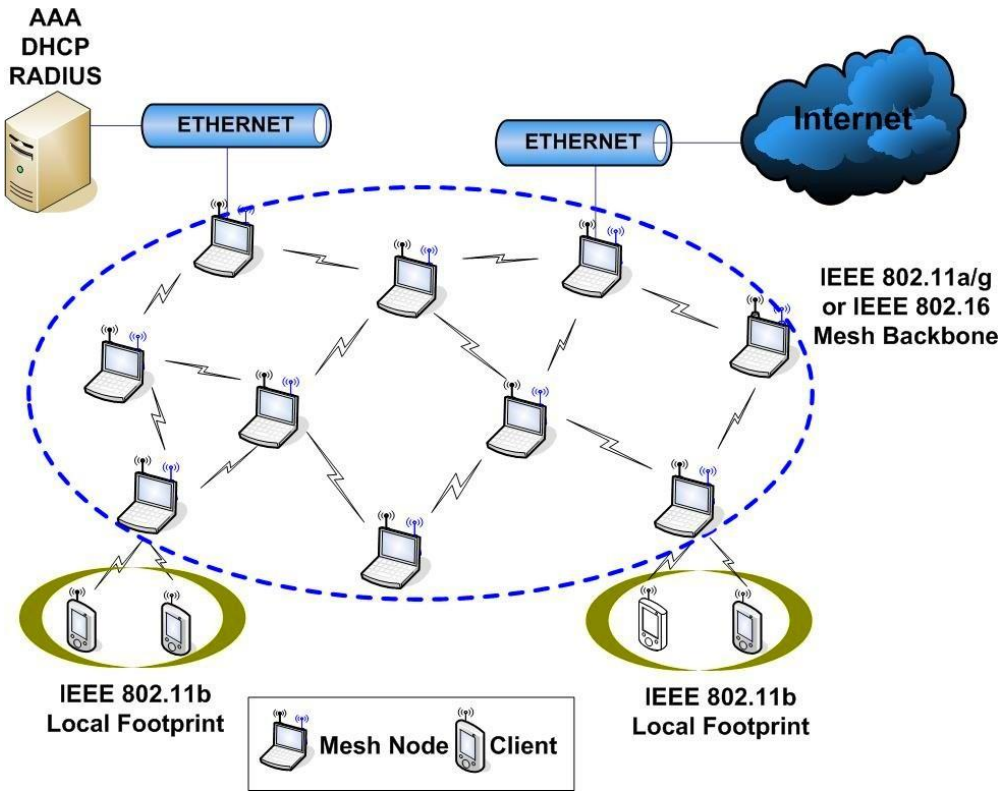

Рисунок 1.3 – Приклад Mesh-мережі

Окремо варто звернути увагу на архітектури, побудовані на основі MESH-мереж. Вони представляють собою децентралізований підхід, у якому кожна роботизована платформа (а подекуди й оператор) виконує функції вузла, здатного не тільки приймати й передавати дані, але й ретранслювати їх для інших вузлів. Така структура створює самоорганізовану та самовідновлювану мережу, що відзначається високою стійкістю до виходу з ладу окремих елементів. Це робить її ідеальною для координації "рою" роботів. Отже, вибір архітектури керування завжди супроводжується пошуком компромісу. Системи P2P забезпечують низьку затримку та автономність, але з обмеженою дальністю. Натомість інфраструктурні системи надають глобальне покриття, проте ціною вищої затримки та залежності від мережі. Саме цей ключовий вибір визначає загальну концепцію проєктування та подальшого вдосконалення систем керування НРП.

1.2 Системи на основі виділених радіоканалів

Визначена раніше архітектура на основі виділених радіоканалів (Point-to-Point, P2P) характеризується прямою лінією зв’язку між оператором та наземною роботизованою платформою (НРП), незалежною від зовнішньої інфраструктури. Така модель стала найпоширенішою для систем телеприсутності завдяки її високій надійності та дуже низькій затримці. Важливим аспектом цієї архітектури є її здебільшого гібридний характер, який передбачає використання двох окремих, паралельних радіоканалів для передачі команд керування (C&C) і відеопотоку. Це рішення обумовлене різними вимогами до цих потоків даних і є ефективним з технічної точки зору. Канал керування вимагає мінімальної пропускної здатності, але основними його характеристиками є максимальна надійність, стійкість до перешкод, велика дальність дії та наднизька затримка. Відеоканал, навпаки, потребує значно більшої пропускної здатності, допускаючи меншу стійкість до перешкод, а його головним пріоритетом залишається мінімізація затримки. У

цьому підрозділі докладно розглядаються принципи функціонування кожного з зазначених компонентів.

Принцип роботи каналу керування на базі LoRa

Реалізація керування на базі LoRa значно розширює можливості сучасних систем радіокерування, особливо для застосувань на великих відстанях. Традиційні вузькосмугові технології вже не забезпечують необхідної ефективності в умовах складного радіоелектронного середовища, що зробило LoRa (Long Range) справжнім проривом. LoRa не є окремим протоколом, а представляє собою фізичний рівень модуляції (PHY), який використовує техніку розширення спектру через лінійну частотну модуляцію (Chirp Spread Spectrum, CSS). Її принцип роботи побудований на передачі даних за допомогою сигналів, частота яких лінійно змінюється (зростає або спадає) з часом, охоплюючи широку смугу частот. Кожному символу в переданих даних відповідає унікальна послідовність таких сигналів.

Рисунок 1.4 – Передавач та приймач ELRS

Ця методика розподіляє енергію сигналу по широкому спектру, забезпечуючи дві ключові переваги. По-перше, LoRa відзначається винятковою стійкістю до перешкод і надзвичайно високою чутливістю

приймача. Завдяки використанню широкого спектру й особливій структурі ЛЧМ-сигналу, система досягає високого коефіцієнта корисного посилення. Це означає, що приймач здатен кореляційною обробкою відокремити корисний сигнал навіть при його рівні нижчому за фон на рівні шуму. Заявлена чутливість до -148 dBm дозволяє підтримувати зв'язок навіть на відстані десятків кілометрів. Другою значною перевагою є низьке енергоспоживання, адже для передачі сигналів на далекі відстані не потрібно застосовувати високу потужність. На основі можливостей LoRa було створено протокол ExpressLRS (ELRS), орієнтований на завдання радіокерування. ELRS максимально адаптує переваги LoRa для потреб RC-керування, де критично важлива мінімальна затримка. Завдяки високій частоті оновлення пакетів (до 500 Гц і більше), а також оптимізованому методу кодування, ELRS забезпечує низьку дискретність керування, що робить роботу платформи більш плавною. Протокол постійно адаптує параметри зв'язку, гарантуючи стабільну затримку в діапазоні 5-20 мілісекунд. Однак LoRa/ELRS має один фундаментальний недолік — дуже низьку пропускну здатність. Ця технологія свідомо жертвує швидкістю передачі даних на користь дальності й надійності. Це є типовим компромісом, описаним у теоремі Шеннона-Гартлі. Пропускна здатність прямо залежить від коефіцієнта розширення спектру (Spreading Factor, SF): чим вищий SF, тим довше сигнал перебуває в ефірі, збільшуючи дальність і надійність передачі, але значно зменшуючи обсяг даних у секунду. У результаті така швидкість передачі, яка зазвичай вимірюється в кіло- або навіть бітах за секунду, достатня лише для трансляції команд керування (наприклад, положення джойстиків чи стану перемикачів) та базової телеметрії (наприклад, координат GPS чи інформації про батарею). Однак передача відеопотоку через LoRa/ELRS технічно неможлива через низьку пропускну здатність.

Принцип роботи каналу відео

Оскільки LoRa не здатен передавати відео, для систем FPV (First-Person View) використовується окрема аналогова технологія. Ця система функціонує за принципом, схожим на роботу аналогових телевізійних передач. Вона складається з бортового відеопередавача (VTX) та наземного відеоприймача (VRX). Передача сигналу відбувається постійно та без цифрової обробки: камера, встановлена на пристрої, генерує композитний аналоговий відеосигнал (зазвичай у форматі PAL або NTSC), який є неперервною електричною хвилею. Цей сигнал містить інформацію про яскравість (luminance), колір (chrominance) та синхронізацію кадрів (sync pulses). Відеосигнал який надходить до VTX, використовується для частотної модуляції (FM) несучої радіочастоти. Таким чином, миттєва напруга вхідного відеосигналу визначає поточну частоту радіохвилі, яка передається в ефір. Наземний VRX приймає сигнал на відповідній частоті, демодулює його (перетворюючи відхилення частоти назад у електричну напругу) і відновлює вихідний відеосигнал PAL/NTSC, який потім подається на монітор або FPV-окуляри.

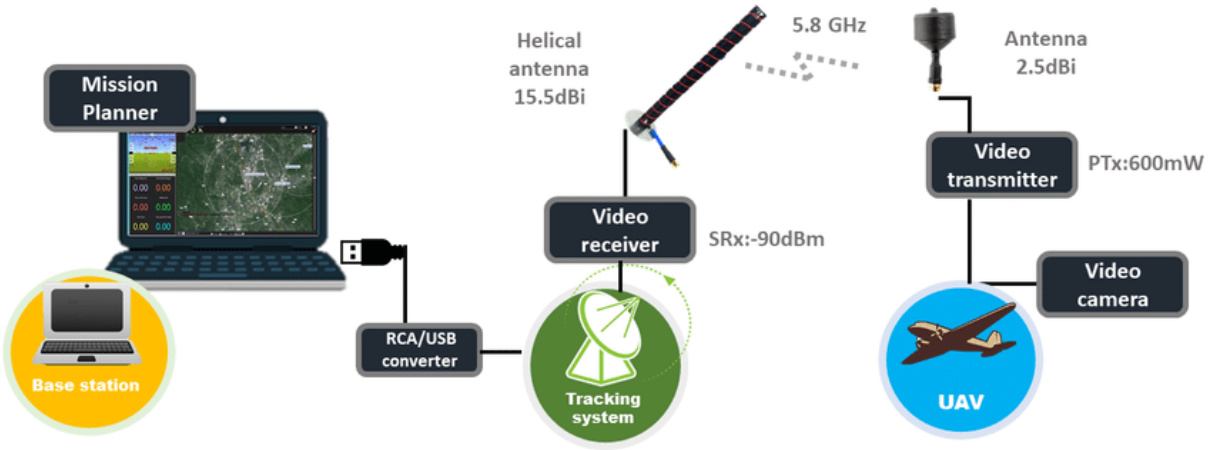

Рисунок 1.5 – Приклад системи відеозв’язку для безпілотників

Головною перевагою цієї технології є практично відсутність затримки в передачі даних. Оскільки формат є повністю аналоговим, процеси, які часто спричиняють затримку в цифрових системах – такі як кодування, стиснення, буферизація, передача пакетів і декодування – тут повністю виключені. Сигнал передається як постійний потік, при цьому затримка "від камери до дисплея" становить лише кілька мілісекунд, залежно від швидкості роботи електронних компонентів та фізичних обмежень, таких як швидкість світла. Ще одним важливим плюсом є плавна деградація сигналу при погіршенні умов прийому. На противагу цифровим системам, які мають "ефект обриву", коли якість зв'язку різко падає і зображення може завмирати або повністю зникати через втрату пакетів даних, аналогова система дозволяє отримати поступове погіршення зображення у вигляді "снігу" або шуму. Таке погіршення виникає через те, що приймач посилює як корисний сигнал, так і фоновий шум одночасно. Це забезпечує оператору цінний зворотний зв'язок щодо стану зв'язку і дає достатньо часу для реагування до моменту повної втрати сигналу.

Основним недоліком аналогового відео є його низька якість зображення (Standard Definition). Роздільна здатність, яка фундаментально визначена стандартами PAL (576i) або NTSC (480i) та обмежена шириною смуги FM-сигналу, не дає змоги оператору розрізняти дрібні деталі, зчитувати текст чи ефективно ідентифікувати об'єкти на середніх і великих відстанях. Ще одним вагомим недоліком є вразливість до перешкод. Система не має механізмів для виправлення помилок і особливо чутлива до багатопроменевого поширення (multipathing), коли приймач одночасно отримує прямий сигнал та його копії, відбиті від різних поверхонь (землі, будівель). Відбиті сигнали досягають приймача з затримкою, що спричиняє фазові спотворення, подвоєння зображення та втрату насиченості кольорів. Вибір робочої частоти є критично важливим для відеопередачі. Найпоширеніший діапазон 5.8 ГГц (5650–5925 МГц) передбачає використання коротких хвиль, що дозволяє застосовувати компактні антени. Однак ці хвилі мають низьку здатність проникати крізь перешкоди та сильно поглинаються або відбиваються такими об'єктами, як

дерева чи стіни будівель, що призводить до значного багатопроменевого ефекту в міських умовах. Натомість частотний діапазон 1.2 ГГц / 1.3 ГГц (1080–1360 МГц) значно краще підходить для наземних платформ. Довші хвилі на цих частотах мають кращу здатність дифрагувати навколо перешкод і проникати крізь об'єкти з меншою щільністю (чагарники, ліс), забезпечуючи стабільну роботу в складних умовах. Це особливо актуально для наземних місій, хоча використання цього діапазону вимагає застосування більших антен.

1.3 Системи на основі глобальних мереж

На відміну від архітектури з виділеними радіоканалами, системи, що функціонують на базі глобальної інфраструктури (Infrastructure-Based), використовують зовсім інший механізм. Вони залежать від наявної комерційної інфраструктури мобільного зв'язку, зокрема мереж 4G (LTE, Long-Term Evolution) та майбутніх перспектив 5G. У цій архітектурі немає прямого радіозв’язку (P2P) між оператором і наземною роботизованою платформою (НРП). Натомість обидві сторони – як НРП, так і операційна станція – виступають незалежними клієнтами в межах глобальної мережі Інтернет. Ця система побудована на принципах цифрової уніфікації. На борту НРП встановлений бортовий комп’ютер, який може бути представленим одноплатними комп’ютерами, такими як Raspberry Pi чи Jetson Nano. До нього підключено периферійні пристрої: камеру, контролер двигунів чи польотний контролер, а також модем 4G/LTE. У свою чергу, оператор має підключення до Інтернету (за допомогою модему або інших засобів), а також станційне програмне забезпечення і пристрої вводу (наприклад, геймпад). Для зв’язку між ними часто використовується сервер VPS як проміжна ланка-ретранслятор, або ж P2P-технології, такі як WebRTC, які намагаються встановити пряме підключення між IP-адресами клієнтів після первинного з’єднання через сервер. Ця архітектура забезпечує уніфіковану передачу всіх потоків даних. На відміну від частково розподілених P2P-підходів, тут не існує

розмежованих каналів для керування і відеопотоків. Усі дані – від відео з камери до телеметрії та команд для керування – передаються у вигляді цифрових IP-пакетів через єдиний 4G-канал. Бортовий комп'ютер НРП постійно захоплює відео, стискає його за допомогою сучасних кодеків, таких як H.264 чи H.265, щоб оптимізувати розмір потоку, і передає його мережею. Паралельно він відстежує вхідні пакети даних із командами керування, які після отримання оперативно передаються на контролер двигунів.

Основною перевагою даної архітектури є можливість забезпечення потенційно необмеженого глобального радіусу дії (Beyond-Line-of-Sight, BLOS). Дальність керування та передача відео залежать не від потужності передавача чи прямої видимості, а виключно від наявності покриття мобільної мережі. Це дає змогу здійснювати управління платформою з будь-якого міста або навіть з іншого континенту. Ще однією важливою перевагою є здатність передавати відео високої чіткості (HD, Full HD і вище), що забезпечується високою пропускною здатністю 4G. Така функція особливо важлива для задач, які потребують детальної ідентифікації об'єктів. Додатково, архітектура характеризується гнучкістю та масштабованістю: відеопотік можна легко поширити до кількох спостерігачів, а керування передавати між різними операторами. Однак такий підхід має й суттєві недоліки, які створюють основні перешкоди для його реалізації. Найсерйознішою проблемою є затримка (latency). На відміну від аналогових каналів зі швидким відгуком, сумарна затримка у 4G-системі є значною, нестабільною і складається з кількох компонентів: часу на кодування відео на борту, затримки передачі даних від пристрою (uplink) до базової станції, обробки в ядрі мережі провайдера, транзиту пакетів через Інтернет (включаючи маршрутизацію і проміжні сервери), передачі на кінцевий пристрій оператора (downlink) та, нарешті, часу декодування сигналу у оператора. У результаті сукупна затримка зазвичай перевищує 100-200 мілісекунд і може досягати декількох секунд у несприятливих умовах. Іншою проблемою є джиттер (jitter), тобто варіативність часу доставки пакетів даних. Через нерівномірність

надходження пакетів стає складно забезпечити плавне відтворення відео, що вимагає використання буферизації. Однак буфери ще більше збільшують загальну затримку, що ускладнює роботу системи.

Третім суттєвим недоліком є залежність від зовнішньої інфраструктури та її функціональної якості. Варто зазначити, що сучасні мобільні мережі не розраховані на обслуговування критичних задач у режимі реального часу. Їхня архітектура оптимізована для асиметричного навантаження, де пріоритетом є високошвидкісне завантаження даних, тоді як швидкість передачі інформації в зворотному напрямку (uplink) залишається меншою. Для роботи додатків, орієнтованих на реальний час (НРП), найбільш важливим аспектом є саме якість і стабільність зворотного каналу передачі даних, який у багатьох випадках перевантажений або позбавлений високого пріоритету. У зонах зі слабким покриттям сигналу або при значному навантаженні на базові станції виникає ризик втрати пакетів даних. Це явище спричиняє феномен "цифрової деградації", який проявляється у вигляді застиглих кадрів (freeze frame), появи артефактів на зображенні, таких як макроблокінг, або у випадках повної втрати зв'язку — так званий "цифровий обрив". Крім того, передача керувальних даних через публічні мережі Інтернет створює значні виклики для забезпечення безпеки, вимагаючи невідкладного впровадження механізмів шифрування, наприклад, використання VPN-технології, з метою захисту інформації від несанкціонованого перехоплення чи модифікації команд.

1.4 Порівняльний аналіз

Попередньо розглянуті підходи окреслили дві принципово різні архітектури для управління наземними роботизованими платформами: класичний гібрид P2P (LoRa + аналогове відео) та інтернет-орієнтовану систему на основі 4G/LTE. Обидві мають свої сильні сторони і критичні недоліки, що визначають їх придатність для конкретних задач. Для того щоб раціонально обрати технологію, на якій базуватиметься поліпшення в цій

роботі, необхідно виконати прямий порівняльний аналіз за основними експлуатаційними та практичними характеристиками. Порівняння затримки та дальності Одними з найважливіших параметрів для будь-якої системи телеприсутності є затримка (яка впливає на можливість керування в режимі реального часу) та дальність (яка визначає діапазон роботи системи).

Таблиця 1.1 - Порівняльний аналіз середньої затримки (Latency)

Архітектура	**Канал Керування (C&C)**	**Канал Відео (Video Feed)**	**Характер затримки**
P2P Гібрид (LoRa + Аналог)	5 – 20 мс	< 10 мс	Стабільна, прогнозована
4G/LTE (Уніфікована)	50 – 200+ мс	150 – 500+ мс	Змінна (Jitter), залежна від мережі

Дані в Таблиці 1.1 наочно показують ключову перевагу гібридної P2P архітектури у питаннях швидкодії. Аналогова передача відео, яка не потребує кодування та буферизації, забезпечує практично миттєвий зворотний зв'язок із затримкою менше 10 мс. Крім того, спеціалізований протокол ELRS (LoRa) забезпечує наднизьку затримку для команд керування в межах 5-20 мс, причому ця затримка є стабільною та передбачуваною завдяки виділеному каналу передачі даних. На відміну від цього, технологія 4G/LTE демонструє значно вищі і, що важливіше, нестабільні показники. Затримка відео включає час на кодування, буферизацію, передачу через мережу та декодування, що загалом становить 150-500+ мс. Затримка керування, у свою чергу, залежить від проходження сигналу через мережу та сервер із "стрибками" (hops), що може досягати 50-200+ мс. Значний джиттер, тобто варіації часу затримки, значно ускладнює процес керування, адже реакція платформи стає непередбачуваною.

Таблиця 1.2 - Порівняльний аналіз операційної дальності (Range)

Архітектура	**Канал Керування (C&C)**	**Канал Відео (Video Feed)**	**Обмежуючий фактор**
P2P Гібрид (LoRa + Аналог)	Дуже велика (10 – 30+ км)	Обмежена (1 – 10 км)	Дальність та якість відео
4G/LTE (Уніфікована)	Глобальна (BLOS)	Глобальна (BLOS)	Покриття мобільної мережі

Таблиця 1.2 демонструє ситуацію, яка є кардинальною протилежністю в контексті дальності комунікаційних каналів. У рамках гібридної P2P системи застосування каналу керування на базі технології LoRa забезпечує виняткову дальність передачі сигналу, що досягає десятків кілометрів, завдяки високій чутливості приймачів. Однак загальна ефективність системи суттєво обмежується дальністю аналогового відеоканалу. Незважаючи на використання низьких частот передачі (1.2 ГГц) і потужних передавачів, максимальна дальність відеосигналу рідко перевищує 10 км, при цьому вона надзвичайно залежить від умов прямої видимості (Line-of-Sight, LOS). Будь-які фізичні перешкоди, такі як будівлі чи пагорби, значно погіршують якість відеосигналу або призводять до його повного блокування. У результаті операційний радіус платформи визначається її найвразливішим компонентом, яким є відеоканал. На противагу цьому, архітектура 4G/LTE здатна усунути обмеження щодо дальності передачі даних. Оскільки система базується на використанні інфраструктури оператора мобільного зв’язку, дальність комунікації стає глобальною (Beyond-Line-of-Sight, BLOS) і залежить виключно від наявності доступного мобільного покриття. Це забезпечує можливість виконання операцій у складних умовах міської забудови або на великих територіях без потреби забезпечення прямої лінії видимості між передавачем і приймачем.

Порівняння на основі практичних критеріїв демонструє значущі аспекти вибору технології з точки зору безпеки та складності реалізації. У контексті забезпечення безпеки системи, архітектура Peer-to-Peer (P2P) гібридного типу виявляє фундаментальну вразливість. Аналоговий відеосигнал на частотах 5.8 ГГц або 1.2 ГГц поширюється у широкомовному режимі, що дозволяє будь-якому користувачу зі стандартним відеоприймачем і знанням робочої частоти здійснити перехоплення відеоструму. Така ситуація є абсолютно неприйнятною у конфіденційних застосуваннях. Хоча механізм керування ELRS використовує унікальний ідентифікатор для зв’язування приймача з передавачем, його функціональність не спрямована на захист від спланованих атак, таких як блокування сигналу або підміна даних. Інша річ — система 4G/LTE, яка базується на IP-протоколі та володіє значно розширеними можливостями щодо безпеки. У той час як сам Інтернет-канал залишається відкритим і публічним, він підтримує використання промислових протоколів шифрування. Одним із найефективніших способів є застосування VPN-технологій, наприклад WireGuard або платформ ZeroTier/Tailscale, що дозволяють створити зашифрований тунель між оператором і безпілотною платформою. Це гарантує конфіденційність даних, включаючи відео та команди управління, які стають недоступними для третіх осіб. Якщо передача здійснюється через WebRTC, то використання стандартного шифрування (DTLS-SRTP) є обов'язковою умовою. Щодо складності реалізації, гібридна P2P система має значно спрощену структуру. Вона складається зі стандартного набору апаратних модулів, таких як приймач ELRS, відеопередавач, відеоприймач і окуляри FPV, і потребує лише базових налаштувань, наприклад вибору частоти або прив’язки компонентів. Цей підхід є типовим прикладом моделі "plug-and-play". З іншого боку, реалізація системи 4G/LTE потребує значно більшого рівня технічної компетентності. Це включає встановлення бортового комп’ютера (SBC), програмну інтеграцію з налаштуванням операційної системи (наприклад, Linux), написання автозапускових сценаріїв та конфігурацію мережевих інтерфейсів і модема LTE через специфічні

команди (AT або MBIM/QMI). Найбільші складнощі виникають при розробці програмного забезпечення для відеообробки і передавання даних, де необхідно налаштувати складні пайплайни для захоплення зображень камерою, апаратного перекодування у формати H.264 або H.265 та стрімінгу за обраними протоколами (RTSP або WebRTC). Додатково потрібне налаштування сервера (VPS) для ретрансляції сигналу або сигналізації WebRTC, що створює суттєві виклики при підтримці системи в робочому стані.

Ціна та розміри обладнання. Компоненти P2P (наприклад, модулі ELRS або аналогові передавачі VTX) є популярними серед хобістів, що робить їх доступними за вартістю (зазвичай в межах кількох десятків доларів) і компактними за розміром. Наземна станція, як-от окуляри чи монітор із приймачем, теж характеризується відносно невисокою ціною. Натомість архітектура 4G/LTE значно дорожча. Бортова частина вимагає застосування одноплатного комп'ютера (SBC), як-от Raspberry Pi 4/5 або Jetson Nano, що обходиться значно дорожче, а також якісного 4G-модема з підтримкою необхідних LTE-діапазонів. Додатково накладаються регулярні операційні витрати: оплата тарифного плану для SIM-карти з великим обсягом вихідного трафіку (необхідного для передачі HD-відео) та щомісячна оренда VPS-сервера у разі його використання в архітектурі. За габаритами, SBC, модем, система живлення та антени займатимуть більше місця і матимуть вищі енергетичні витрати порівняно з компактними P2P-модулями. Обґрунтування вибору 4G/LTE Аналіз демонструє суттєвий компроміс між двома підходами. P2P-архітектура забезпечує високу продуктивність завдяки низькій затримці, однак має принципові обмеження: низьку якість відео, малу дальність дії при прямій видимості (LOS) та відсутність захисту даних. Ці обмеження є фізичними властивостями аналогового зв'язку і не можуть бути компенсовані програмно. На противагу цьому, архітектура 4G/LTE пропонує високу функціональність: глобальну дальність зв'язку, HD-якість відео та високий рівень безпеки. Але вона має свої проблеми – висока й мінлива затримка, що негативно впливає на продуктивність. Для цілей даної дипломної роботи, що

передбачає "дослідження та вдосконалення", архітектура 4G/LTE є більш релевантною через її науковий і практичний потенціал. Її недоліки здебільшого не є фізичними, а зумовлені програмними та алгоритмічними аспектами. Це створює значні можливості для оптимізації через вдосконалення програмного забезпечення, використання ефективних протоколів (наприклад, WebRTC замість RTSP-over-TCP), динамічне регулювання бітрейту залежно від стану каналу і розробку алгоритмів компенсації затримки та прогнозування. Таким чином, технологія 4G/LTE обирається як основа для подальшої реалізації та дослідження. Завданням роботи буде не лише створення чергової системи на базі 4G, а впровадження методів, спрямованих на подолання її недоліків, зокрема затримок і нестабільності. Мета полягає у наближенні експлуатаційних характеристик до рівня P2P-систем при збереженні ключових переваг 4G/LTE – глобальної дальності, безпеки й високої якості відео.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ СИСТЕМ КЕРУВАННЯ ЧЕРЕЗ ГЛОБАЛЬНУ МЕРЕЖУ

2.1 Архітектурні моделі IP-керування

Перехід до використання глобальних мереж 4G/LTE, як було обґрунтовано раніше, суттєво трансформує концепцію зв'язку. Замість прямого з'єднання Point-to-Point виникає взаємодія між двома клієнтами — наземною роботизованою платформою (НРП) і станцією оператора, які функціонують у межах публічної мережі Інтернет. Основна проблема полягає в тому, що ці клієнти зазвичай не мають "білих" (публічних) IP-адрес і розташовані за NAT (Network Address Translation). Мобільні оператори надають пристроям (модемам) приватні IP-адреси з внутрішнього пулу, що унеможливлює прямий доступ до НРП, адже її адреса залишається недоступною з глобальної мережі. Те ж саме часто стосується й оператора, який може підключатися через домашній Wi-Fi роутер. Для організації IP-з'єднання між ними необхідно

впроваджувати одну з двох базових архітектурних моделей: клієнт-сервер або Peer-to-Peer.

Архітектура клієнт-сервер є однією з найпоширеніших і найзручніших для впровадження моделей. Її основна ідея полягає у використанні проміжного публічного сервера (VPS/VDS) зі статичною публічною (білою) IP-адресою. Цей сервер виконує роль посередника або ретранслятора. Принцип роботи моделі базується на простих взаємодіях. Після увімкнення і підключення до мережі 4G, НРП встановлює вихідне з'єднання з наперед відомою публічною IP-адресою сервера. Оскільки це вихідне з'єднання, мобільний NAT безперешкодно дозволяє його. Одночасно станція оператора також з'єднується із сервером. У результаті сервер отримує дані про обидві сторони і стає посередником: оператор надсилає команди серверу, а той передає їх НРП через вже існуюче з'єднання.

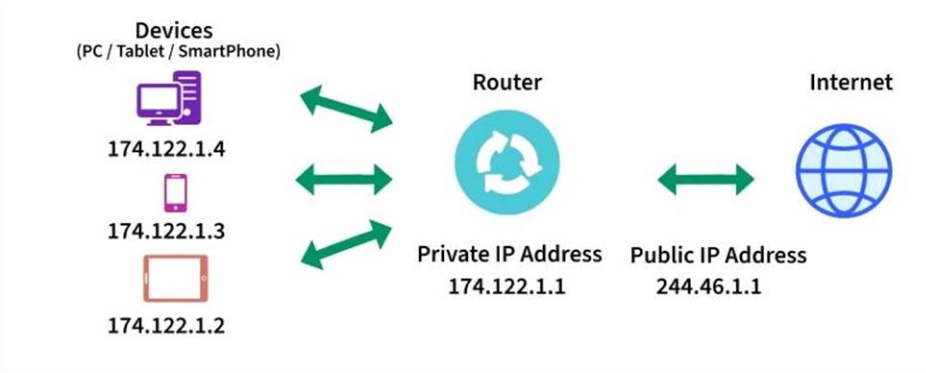

Рисунок 2.1 – Приклад NAT

Аналогічно відбувається передача відеопотоків та телеметрії у зворотному напрямку. Переваги архітектури клієнт-сервер включають її високу надійність і простоту реалізації. Система стабільно працює навіть із різними типами NAT, оскільки вона потребує лише вихідних запитів, які майже завжди підтримуються. Це виключає необхідність складних механізмів для обходу NAT. Однак є і певні недоліки, пов'язані з особливостями цієї архітектури. Найбільшим мінусом є збільшення затримки. Дані проходять

через сервер, що подвоює шлях: від НРП до сервера, а потім – від сервера до оператора. Рівень затримки залежить від місця розташування сервера. Додатково сервер стає критично важливим елементом системи – його вихід із ладу призводить до повної втрати керування платформами (Single Point of Failure). Крім того, на нього лягає весь трафік взаємодії, що потребує високої пропускної здатності каналу зв’язку сервера.

Архітектура Peer-to-Peer (P2P) є значно складнішою в порівнянні з клієнт-серверною моделлю, проте вона спрямована на вирішення її головного недоліку — ретрансляції. Основна мета P2P полягає у встановленні прямого з'єднання між кінцевим користувачем і оператором, що дозволяє передавати дані найкоротшим маршрутом без залучення проміжного сервера. Через те, що обидва клієнти зазвичай знаходяться за NAT, для організації такого з'єднання застосовуються спеціалізовані технології, які входять до складу протоколу ICE (Interactive Connectivity Establishment). ICE, своєю чергою, є ключовим компонентом WebRTC (Web Real-Time Communication).

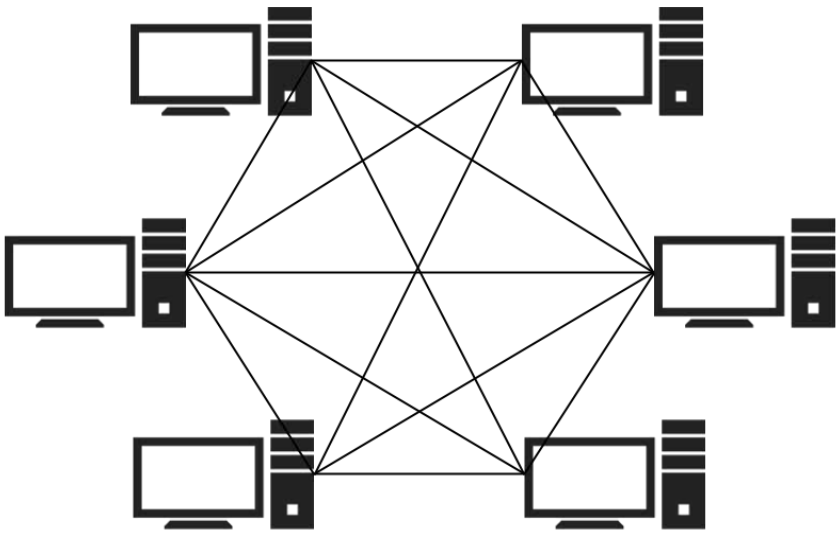

Рисунок 2.2 – Приклад P2P

Процес роботи P2P складається з кількох етапів. Спочатку обидва клієнти підключаються до публічного сигнального сервера, що потрібен лише для того, щоб вони могли надати одне одному необхідну службову інформацію. Далі клієнти звертаються до STUN-сервера, який повідомляє їм їхні публічні IP-адреси та порти, що були призначені NAT. Після обміну цими даними через сигнальний сервер клієнти намагаються налагодити пряме з'єднання — цей процес відомий як NAT traversal. Якщо пряме з'єднання все ж неможливо налаштувати (наприклад, через складний симетричний NAT), механізм ICE автоматично переходить на альтернативне рішення — використання TURN-сервера. TURN-сервер фактично виконує функцію ретранслятора і працює за принципом клієнт-серверної архітектури. Основною перевагою P2P-архітектури є можливість забезпечення мінімальної затримки під час передачі даних у разі успішного обходу NAT, оскільки пакети рухаються напряму. Проте недоліками цієї моделі залишаються її технічна складність у реалізації та відсутність абсолютної гарантії прямого з'єднання. Ефективність механізмів STUN/TURN значною мірою залежить від налаштувань й обмежень мобільних операторів. У багатьох випадках, особливо зі складними симетричними NAT у мережах 4G, встановити пряме P2P-з'єднання стає неможливо, і система змушена вдаватися до ретрансляції через TURN-сервер, що анулює основні переваги архітектури.

2.2 Аналіз протоколів передачі відеопотоку в реальному часі

Після визначення загальної архітектурної моделі з'єднання, чи то клієнт-сервер, чи P2P, одним із ключових завдань, що безпосередньо впливає на ефективність роботи системи, є вибір протоколу передачі відеопотоку. Саме відеопотік створює основне навантаження на канал 4G, і швидкість його доставки визначає значну частину загальної затримки між камерою та оператором. У середовищі 4G-мереж з нестабільними умовами—змінною пропускною здатністю та ймовірними втратами пакетів—звичайні стрімінгові протоколи не здатні забезпечити прийнятну якість передачі. Перед тим як

перейти до аналізу протоколів, важливо врахувати роль відеокодеків, адже вони є основою всієї системи. "Сирий" відеопотік, що надходить безпосередньо від камери, має величезний обсяг даних, іноді досягаючи кількох гігабіт на секунду, що робить його непридатним для передачі через мережу 4G. Тому обов’язковим є його стиснення. Найчастіше використовується кодек H.264 (AVC), який забезпечує хороший баланс між рівнем стиснення та складністю обробки. Водночас сучасніший кодек H.265 (HEVC) демонструє значно вищу ефективність: він дозволяє отримати аналогічну якість відео при приблизно удвічі меншому бітрейті або досягнути кращої якості зображення за тих самих параметрів бітрейту. Для 4G-мереж, де пропускна здатність, особливо на передачу даних (uplink), є критично важливим ресурсом, застосування H.265 виглядає дуже перспективним. Однак слід враховувати, що його використання потребує потужнішого обладнання для реального часу кодування відеопотоку на бортовому комп'ютері.

Таблиця 2.1 – Порівняння необхідної смуги пропускання для кодеків H.264/H.265

Розширення	**H.264/AVC**	**H.265/HEVC**
480p	1.5 Mbps	0.75 Mbps
720p	3 Mbps	1.5 Mbps
1080p	6 Mbps	3 Mbps
4K	32 Mbps	15 Mbps

RTSP, або протокол потокової передачі в реальному часі, є одним із найстаріших і найпоширеніших у сфері відеоспостереження. Його головна функція полягає не в передачі відеоданих, а у керуванні потоками через набір команд, таких як SETUP, PLAY, PAUSE та TEARDOWN. У цьому сенсі RTSP можна порівняти з "пультом дистанційного керування". Сам медіа-потік, закодований за допомогою кодеків H.264 або H.265, передається окремо з використанням протоколу RTP. Однією з основних задач RTSP є вибір транспортного протоколу для передачі RTP-даних. Спочатку RTSP

підтримував як UDP, так і TCP. Використання UDP забезпечує високу швидкість передачі, оскільки пакети надсилаються без перевірки їх отримання. Якщо пакет загублений у мережі 4G, він просто пропадає, що може спричинити короткочасні артефакти у відео, наприклад "розсипання" зображення. Проте потік продовжує функціонувати, хоча цей метод є менш надійним. Складнощі виникають, коли RTSP працює через TCP, часто для обхідного проходження через фаєрволи. TCP забезпечує гарантовану доставку даних, але може стати перешкодою для передачі у реальному часі через проблему "блокування початку черги" (Head-of-Line Blocking). У такому випадку при втраті одного пакета вся передача припиняється до його повторного відправлення. В мережах 4G це може спричинити кількасекундне "зависання" відео, що унеможливлює ефективне керування відеопотоком.

WebRTC (Web Real-Time Communication) є не просто протоколом, а цілісним програмним фреймворком, створеним Google для забезпечення зв'язку в реальному часі прямо у веб-браузерах. Водночас завдяки своїй універсальності та відкритості, він став фактичним стандартом для будь-яких задач P2P-комунікації, включно з робототехнікою. WebRTC пропонує широкий набір технологій із "коробки": механізми ICE, STUN та TURN для подолання перешкод NAT, обов’язкове шифрування потоків (SRTP), а також протоколи передачі даних (SCTP).

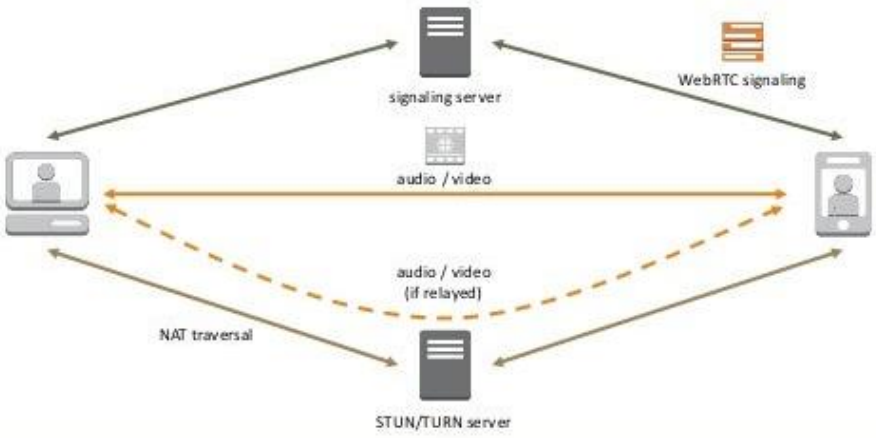

Рисунок 2.3 – Схема з’єднання за допомогою WebRTC

Особливу перевагу WebRTC забезпечує у 4G-системах завдяки вбудованому механізму адаптивного керування бітрейтом (Adaptive Bitrate Control). WebRTC безперервно аналізує стан каналу зв’язку: визначає затримку (RTT), відсоток втрат пакетів та доступну пропускну здатність. Якщо якість мережі 4G падає (наприклад, пристрій опиняється в зоні зі слабким сигналом), WebRTC оперативно дає команду кодеку H.264 знизити якість відео шляхом зменшення бітрейту. Це може спричинити тимчасове погіршення чіткості зображення, але при цьому зберігаються ключові показники – низька затримка та безперервність потоку. Як тільки з'єднання покращується, WebRTC автоматично відновлює вищий бітрейт. Ця здатність до адаптації робить його ідеальним вибором для роботи в умовах нестабільних мобільних мереж.

SRT (Secure Reliable Transport) – це сучасний протокол з відкритим кодом, розроблений для вирішення викликів, пов'язаних зі стрімінгом у ненадійних та нестабільних мережах. Його концепція полягає в об'єднанні переваг TCP і UDP: забезпечення надійності TCP при збереженні низької затримки, характерної для UDP. Працюючи на основі UDP, SRT додає свій вдосконалений механізм автоматичного відновлення втрачених пакетів (ARQ – Automatic Repeat Request).

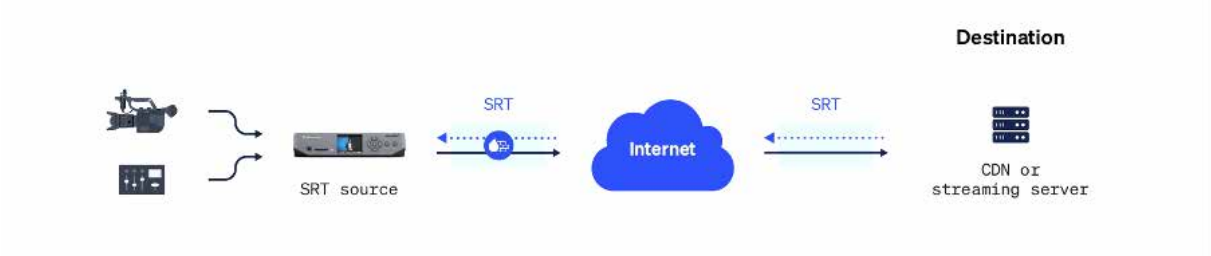

Рисунок 2.4 – Схема з’єднання за допомогою SRT

На відміну від TCP, який припиняє передачу в разі втрати даних, SRT продовжує відправляти потік. Якщо приймач виявляє пропущений пакет за його номером, то надсилається запит на повторну відправку лише цього конкретного пакета. Цей процес відбувається паралельно з основною передачею даних. Для роботи цього механізму SRT використовує буфер затримки, який можна налаштувати. Наприклад, можна встановити допустиму затримку на рівні 200 мс. Це забезпечує протоколу часовий інтервал у 200 мс для виявлення втрати, запиту повторної передачі та отримання втраченого пакета до моменту його відображення. Завдяки цьому SRT є надзвичайно надійним навіть у випадках високого рівня втрат пакетів, що часто зустрічається в мережах 4G, при цьому зберігаючи стабільну та помірно низьку затримку. Додатково, протокол оснащений вбудованим шифруванням AES із початкової конфігурації.

2.3 Аналіз протоколів для передачі команд та телеметрії

У системі керування на базі 4G/LTE, крім ключового відеопотоку, що вимагає високої пропускної здатності, необхідно одночасно і стабільно обробляти ще два типи даних. Перший тип — це команди керування, які оператор передає до наземного або повітряного пристрою (норми переміщення джойстиків, активація кнопок). Другий тип — потік телеметрії, який надходить у зворотному напрямку і містить дані про GPS-координати, заряд батареї, швидкість, а також інші діагностичні показники. На відміну від обсягів відеоданих, ці потоки мають значно менший розмір, але їх обробка вимагає спеціальних технічних умов. Команди керування повинні мати найменшу затримку та високу частоту оновлення (наприклад, 20-50 разів за секунду). При цьому невелика втрата окремого пакета даних не є критичною, якщо наступний пакет надійде протягом 20 мс. Потік телеметрії менше залежить від затримки, проте важливі дані (як-от попередження про низький рівень заряду) повинні бути гарантовано доставленими. Вибір відповідного транспортного

протоколу для цих потоків даних є не менш важливим завданням, ніж підбір оптимального рішення для відео.

TCP (Transmission Control Protocol) є протоколом, орієнтованим на встановлення з'єднання, який фактично став стандартом для переважної більшості інтернет-трафіку, включаючи веб-сторінки та електронну пошту. Його ключова перевага полягає в гарантованій доставці даних. Для досягнення цієї мети TCP використовує механізми підтвердження передачі (ACK), контроль потоку та повторну передачу (retransmission), забезпечуючи, що кожен байт інформації буде доставлений отримувачу у правильному порядку. З першого погляду така надійність здається привабливою для управління командними системами. Проте на практиці TCP є одним із найгірших варіантів для керування в реальному часі. Причина, через яку цей протокол мало придатний для потоків відео, особливо гостро проявляється й у цій сфері — явище "блокування початку черги" (Head-of-Line Blocking). Уявімо ситуацію: оператор використовує джойстик і надсилає командні дії зі швидкістю 50 повідомлень за секунду. Якщо в 4G-мережі буде втрачено один пакет (наприклад, команду "рух вперед на 50%"), TCP зупинить передачу всіх наступних команд. Жодна з більш актуальних команд ("рух вперед на 60%", "стоп") не зможе бути передана доти, доки втрачену команду "рух вперед на 50%" не буде успішно відправлено повторно. Внаслідок цього, через затримку, отримувач може отримати застарілу команду, що може призвести до непередбачуваних і потенційно небезпечних наслідків. Отже, забезпечення гарантованої доставки TCP, яке є його перевагою у багатьох випадках, стає критичним недоліком у контексті систем управління (C&C).

UDP (User Datagram Protocol) повністю протилежний TCP. Це протокол без встановлення з'єднання, який діє за принципом "відправив і забув". Він не гарантує доставки, не має механізмів повторної передачі даних і не забезпечує порядок прибуття пакетів. Його робота зводиться до того, щоб якнайшвидше відправити пакет даних (датаграму) за вказаною адресою. Такі особливості

роблять UDP ідеальним вибором для команд управління C&C. Головна його перевага – мінімальні затримки. Нові пакети команд ніколи не утримуються через невчасну обробку старих. Наприклад, якщо якийсь із пакетів (на кшталт команди "рухатися вперед на 50%") губиться у 4G-мережі, він просто зникає. Це несуттєво, адже через 20 мілісекунд операторська станція вже відправить черговий, більш актуальний пакет (наприклад, "рухатися вперед на 52%"). У системах управління пріоритетною завжди є найсвіжіша команда, а не застаріла, навіть якщо її доставлено гарантовано. Тому невеликий рівень втрат пакетів, властивий 4G-мережам, є прийнятною ціною за миттєву реакцію. Завдяки цьому UDP виступає оптимальним рішенням для C&C-потоків, забезпечуючи необхідну швидкість і чутливість системи.

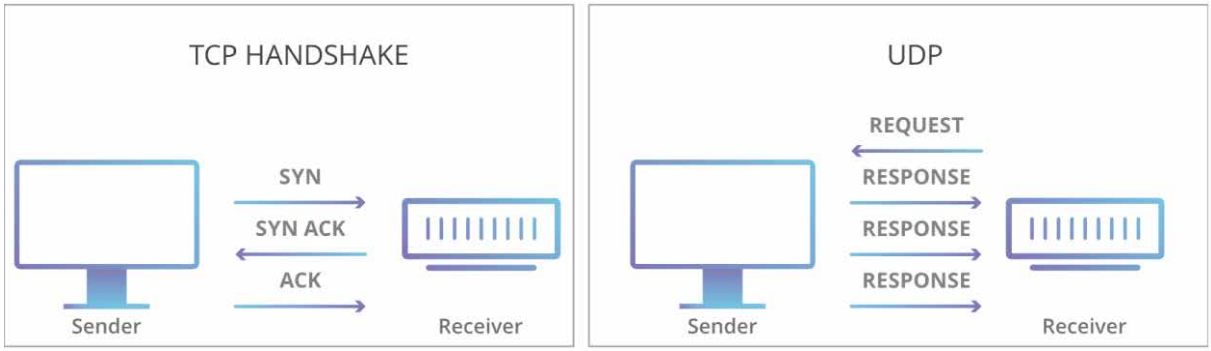

Рисунок 2.5 – Принцип роботи TCP та UDP

MQTT (Message Queuing Telemetry Transport) є протоколом прикладного рівня, створеним спеціально для роботи в середовищі "Інтернету речей" (IoT) і передачі телеметричних даних. Це не транспортний протокол, як TCP або UDP, але він функціонує поверх TCP, використовуючи модель взаємодії "видавець-підписник" (Publish-Subscribe). Основний принцип роботи MQTT полягає у використанні "брокера" (сервера), який оперує "темами" (topics), такими як ugv/gps/location або ugv/battery/voltage. Один клієнт (наприклад, пристрій) "публікує" свої дані (наприклад, GPS-координати) у відповідній темі

на брокері. Інший клієнт, наприклад, операторська станція, "підписується" на цю тему та майже миттєво отримує всі оновлення, які публікуються.

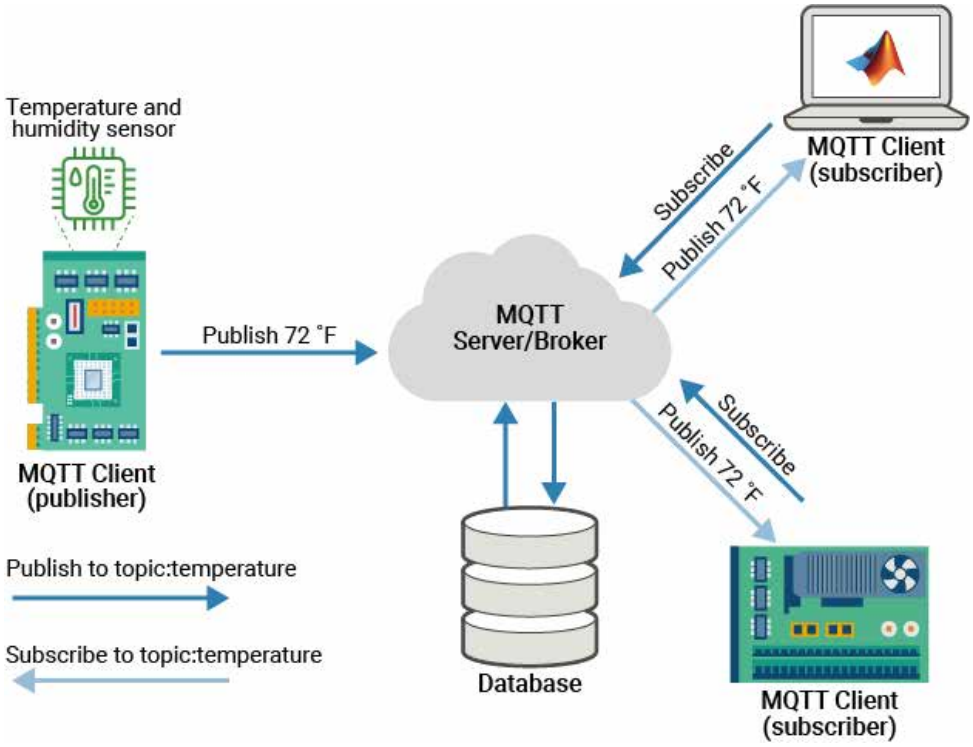

Рисунок 2.6 – Приклад роботи MQTT

Цей протокол є чудовим вибором для телеметрії завдяки своїй легкості та ефективності. Він має мінімальне навантаження в заголовках, що знижує обсяг необхідного трафіку. Модель Pub/Sub дозволяє підключати кілька спостерігачів одночасно, наприклад, оператора, логістичний центр чи розробника, які всі мають доступ до актуальних телеметричних даних. Крім того, MQTT пропонує налаштування рівня "якості обслуговування" (QoS), яке забезпечує підвищену надійність завдяки TCP-основі — наприклад, для гарантованої доставки критично важливих повідомлень на кшталт системних помилок. Проте через залежність від TCP і проміжного брокера MQTT не є оптимальним вибором для реалізації команд керування (C&C). Це пов'язано з тією ж проблемою затримок, яка характерна для чистого TCP.

2.4 Огляд програмно-апаратного стеку

Попередній аналіз архітектурних моделей, відеопротоколів та протоколів керування формує теоретичну основу. Для практичного створення системи керування на основі 4G/LTE використовується певний програмно-апаратний стек. У цьому підрозділі описані основні компоненти, які часто застосовуються для реалізації таких систем, подібних до тієї, що буде розглянута в наступному розділі.

Апаратна частина: Бортовий комп'ютер і модем Ключовим елементом бортової системи НРП є одноплатний комп'ютер (SBC), що служить керуючим вузлом. Він відповідає за кодування відео, виконання логічних операцій і мережеву взаємодію.

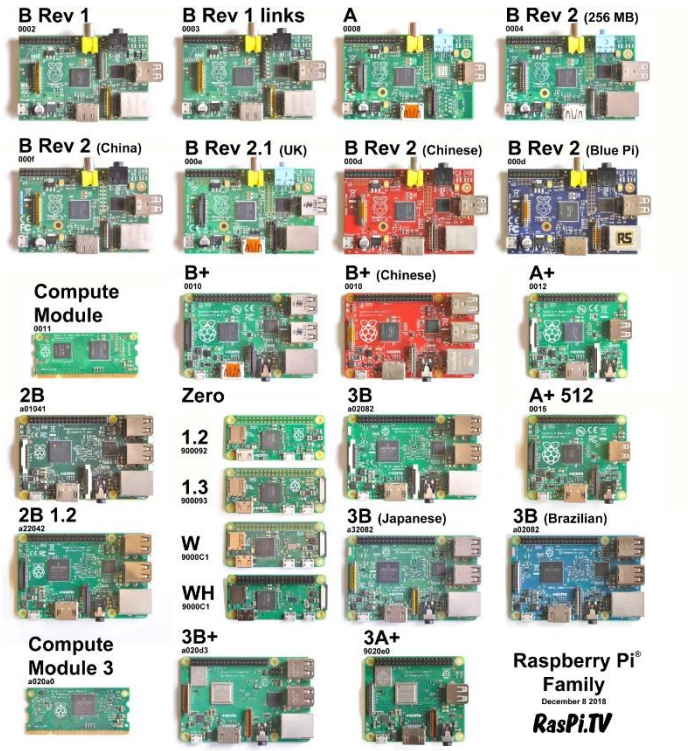

Рисунок 2.7 – Сімейство мікрокомп’юторів Raspberry Pi

Часто перевага надається платформам Raspberry Pi (зокрема Pi 4 Model B), які забезпечують оптимальний баланс між продуктивністю, енергоефективністю та можливістю апаратного стиснення відео. Для підключення до інтернету широко застосовуються 4G/LTE USB-модеми, наприклад, моделі Huawei E3372 або промислові аналоги від Quectel і Sierra Wireless. Живлення цих компонентів забезпечується за допомогою регуляторів напруги (BEC), що підключаються до бортової батареї. Програмна частина: Керування та відеопередача Основою програмного середовища одноплатного комп'ютера в більшості випадків залишається операційна система Linux (наприклад, Raspberry Pi OS), яка дозволяє повністю контролювати як мережевий, так і апаратний функціонал. Для передачі команд керування і телеметрії за протоколом MAVLink використовується утиліта MAVProxy. Вона створена на базі Python і може слугувати клієнтом для обміну даними з летючим контролером через UART або працювати як ретранслятор у серверному середовищі. Для обробки та передачі відеопотоку застосовуються такі інструменти, як GStreamer або ffmpeg. Ці фреймворки дозволяють захоплювати відео зі встановленого джерела (наприклад, IP-камери чи тестового джерела), стискати його (якщо потрібно) або передавати в готовому форматі через мережу за RTSP-протоколом. У серверному середовищі для прийому та ретрансляції відеопотоків поширені легкі медіа-сервери, як-от open-source рішення mediamtx (rtsp-simple-server). Серверна платформа й автоматизація Згідно з аналізом у підрозділі 2.1, для вирішення проблеми CG-NAT необхідно мати хостинг із постійною публічною IP-адресою як точку входу до системи. Для цього часто залучають хмарні інфраструктури від провайдерів, як-от AWS EC2 (Amazon Web Services). Це дає змогу створити віртуальний сервер із закріпленою публічною IP-адресою (Elastic IP) та налаштуванню правил доступу (Security Groups), які відкриватимуть потрібні порти (наприклад, UDP для MAVProxy або TCP/UDP для RTSP).

Для забезпечення стабільної роботи та автоматичного запуску процесів, зокрема ретрансляторів mavproxy і mediamtx на сервері, а також клієнтських

скриптів mavproxy-client і ffmpeg-stream на Raspberry Pi, у середовищі Linux застосовується системний менеджер systemd. Цей інструмент дає змогу створювати конфігураційні файли .service, які визначають правила запуску, перезапуску та управління залежностями фонового виконання процесів.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ СИСТЕМИ КЕРУВАННЯ

3.1 Розгортання та налаштування серверної інфраструктури

Теоретичний аналіз, проведений у Розділі 2, продемонстрував, що для подолання фундаментальної проблеми CG-NAT (Carrier-Grade NAT) , яка унеможливлює пряме з'єднання між НРП та наземною станцією, необхідне впровадження проміжного сервера-посередника . Цей сервер повинен мати статичну публічну IP-адресу і виступати в ролі "точки зустрічі" для обох клієнтів. Спираючись на результати аналізу програмно-апаратних платформ (підрозділ 2.4), для впровадження серверної інфраструктури було обрано платформу Amazon Web Services (AWS), а саме сервіс Elastic Compute Cloud (EC2). Вибір цієї платформи обґрунтовано її високою надійністю, можливістю отримання постійної статичної IP-адреси (Elastic IP) і наявністю гнучких інструментів для налаштування системи захисту (Security Groups). У межах проведеного дослідження використано рівень Free Tier, що дозволив розгорнути сервер t2.micro, який забезпечує достатню продуктивність для ретрансляції трафіку MAVLink та передачі відео.

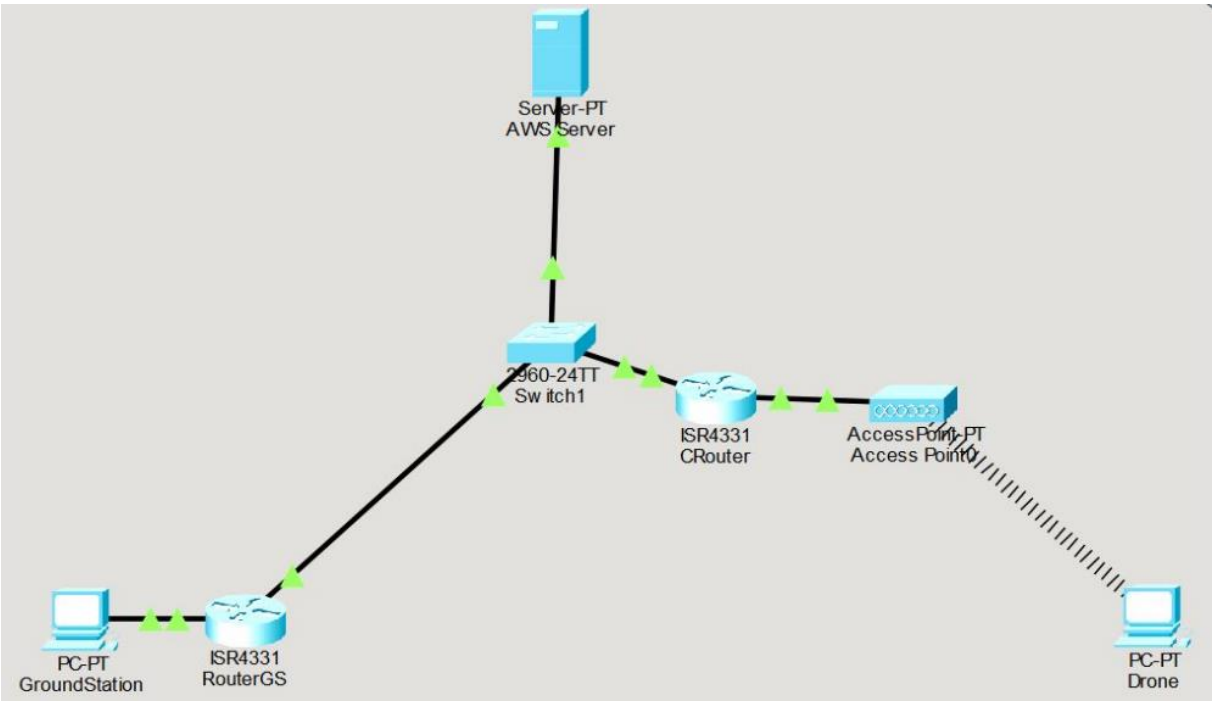

Рисунок 3.1 – Модель системи реалізована в симуляторі

Процес розгортання серверної інфраструктури складався з трьох ключових етапів, реалізованих за допомогою консолі управління AWS.

Етап 1: Створення віртуального сервера (EC2 Instance). На першому етапі було запущено новий екземпляр EC2. Для операційної системи обрали Ubuntu Server 24.04 LTS — стабільну, поширену і добре документовану платформу. Тип екземпляра визначено як t2.micro, оскільки він включений до Free Tier і має відповідні ресурси (1 vCPU, 1 GB RAM) для задач з низьким завантаженням, таких як ретрансляція. У процесі налаштування була створена та завантажена ключова пара у форматі .pem. Цей ключ є критично важливим для безпечного доступу до сервера через SSH, який використовувався для подальшого встановлення необхідного програмного забезпечення.

Етап 2: Налаштування брандмауера (Security Groups). Цей етап був ключовим у забезпеченні мережевої конфігурації та безпеки. В AWS Security Groups виконують роль віртуального брандмауера, керуючи вхідним і вихідним трафіком. Було створено нову групу безпеки з налаштуванням

правил вхідного трафіку. Спочатку додали правило для SSH (TCP/порт 22), що дозволяло адміністративний доступ. З міркувань безпеки джерело для цього правила обмежили параметром My IP, дозволяючи підключення лише з актуальної IP-адреси розробника. Наступне правило стосувалося Custom UDP на порті 14550 з джерелом Anywhere (0.0.0.0/0). Воно забезпечувало отримання сервером MAVProxy телеметрійних і керівних UDP-пакетів від НРП та GCS, чиї IP-адреси можуть бути динамічними та невідомими заздалегідь. Пізніше, під час налаштування відеотрансляції, Security Group було розширено. Додано правило для Custom TCP на порту 8554, необхідного для обробки сигнальних команд протоколу RTSP. Також відкрили діапазон портів 8000-8001 за допомогою правила Custom UDP. Це рішення виявилося критично важливим, адже протокол RTSP окремо використовує ці порти для відеопотоку (RTP) і контрольних пакетів (RTCP). Відсутність налаштувань для порту 8001 спочатку викликала розриви з'єднання (Broken pipe) кожні 10 секунд після запуску трансляції, оскільки сервер mediamtx не отримував контрольних пакетів.

Етап 3: Призначення статичної IP-адреси (Elastic IP). У момент запуску інстансу EC2 йому надається динамічна публічна IP-адреса, яка може змінитися після перезавантаження. Така поведінка адресації є неприйнятною для серверної архітектури, де необхідна стабільність мережевої доступності. З метою забезпечення постійної точки доступу було використано сервіс AWS Elastic IP. У рамках роботи з консольною платформою EC2 було здійснено виділення нової Elastic IP-адреси, яка мала значення 16.16.174.134. Далі відбувся процес асоціювання цієї статичної IP-адреси із запущеним інстансом. Завершення виконання описаних трьох етапів дозволило одержати повністю сконфігурований, безпечний, завдяки обмеженням SSH-доступу, сервер, який підтримує стабільну мережеву доступність через постійну публічну IP-адресу. Інфраструктура була готова до подальшого встановлення та налаштування програмного забезпечення для ретрансляторів MAVProxy і mediamtx, що детально описано у наступному розділі.

3.2Налаштування серверного програмного забезпечення

Після завершення розгортання і налаштування хмарної інфраструктури AWS наступним етапом стала установка та конфігурація серверного програмного забезпечення. Це програмне забезпечення виконує критично важливу функцію ретрансляції для двох незалежних потоків даних: команд управління MAVLink та відеопотоку RTSP. Для забезпечення адміністрування сервера застосовувався SSH-клієнт PuTTY, що дозволив встановити безпечне з'єднання з екземпляром EC2, використовуючи попередньо створений ключ .pem (конвертований у формат .ppk для PuTTY) та Elastic IP-адресу 16.16.174.134. Налаштування системи ретрансляції MAVProxy (управління та телеметрія) Для організації передачі трафіку MAVLink (команди управління і телеметрія) була використана утиліта MAVProxy, вибір якої аргументовано в розділі 2.4.

1. Установка MAVProxy Програму було встановлено на сервері під управлінням операційної системи Ubuntu. Спочатку виконувалося оновлення пакетів (команда: sudo apt update) та установка менеджера пакетів Python (команда: sudo apt install python3-pip). Однак при встановленні виникла проблема сумісності через те, що в Ubuntu 24.04 заборонено пряме встановлення пакетів через pip з метою уникнення конфліктів із системними бібліотеками. Цю проблему вдалося вирішити завдяки інсталяції pipx — інструмента, який забезпечує установку Python-додатків в ізольованих середовищах. Встановлення MAVProxy було успішно проведено за допомогою відповідних команд.

Після цього виникла проблема відсутності залежності (ModuleNotFoundError: No module named 'future'), яку було вирішено "впровадженням" (inject) відсутнього пакету безпосередньо в ізольоване середовище MAVProxy. Після цього MAVProxy був готовий до роботи.

2. Автоматизація MAVProxy за допомогою systemd. Для забезпечення стабільної роботи ретранслятора (цілодобово, 24/7) та його автоматичного запуску після перезавантаження сервера був створений systemd сервіс. Для цього підготували конфігураційний файл за адресою sudo nano /etc/systemd/system/mavproxy.service. Під час налаштування сервісу виявили кілька проблем, які потребували поступового вирішення:

Проблема 1: Помилка "Permission denied". Журнал journalctl вказав, що MAVProxy не може створити лог-файл (mav.tlog), оскільки systemd запускає процес із кореневого каталогу (/), до якого користувач ubuntu не має прав на запис.

Рішення 1: У конфігураційний файл .service була додана директива WorkingDirectory=/home/ubuntu, яка змусила процес починати роботу з домашньої директорії, де прав на запис достатньо.

Проблема 2: Процес не запускався з автоматичним перезапуском (auto-restart). Виведення journalctl показало, що MAVProxy розпочинає роботу, але одразу завершується. Це трапляється тому, що MAVProxy є інтерактивною програмою, яка потребує наявності терміналу. Під час запуску за допомогою systemd у фоновому режимі MAVProxy не бачить терміналу і завершує роботу.

Рішення 2: До команди запуску був доданий прапор --daemon, який дозволив MAVProxy працювати у фоновому режимі без прив’язки до інтерактивного терміналу.

Після активації сервісу за допомогою команд sudo systemctl daemon-reload, sudo systemctl enable mavproxy.service і sudo systemctl start mavproxy.service, система успішно запустила його у фоновому режимі. Сервіс почав прослуховувати UDP-порт 14550.

Налаштування ретранслятора mediamtx (відеопотік) Для ретрансляції відеопотоку було вирішено використовувати сервер mediamtx (раніше відомий як rtsp-simple-server) завдяки його простоті й ефективності.

Процес інсталяції здійснено шляхом завантаження готового бінарного файлу з офіційного GitHub-репозиторію проєкту. У подібний спосіб до налаштування MAVProxy, для забезпечення автоматичного запуску mediamtx було створено файл сервісу systemd. Для цього використали команду sudo nano /etc/systemd/system/mediamtx.service. Після активації цього сервісу серверна частина була повністю налаштована, автоматизована та готова до прийому з'єднань від НРП та GCS як для керування, так і для відеотрансляції.

3.3Налаштування бортового комп’ютера

Бортовий комп’ютер виконує важливу функцію, забезпечуючи апаратно-програмну взаємодію між фізичним обладнанням НРП, таким як польотний контролер та камера, і хмарною серверною інфраструктурою. Для реалізації цього компонента, базуючись на аналізі, проведеному в розділі 2.4, було обрано одноплатний комп’ютер Raspberry Pi 4 Model B.

Процес його налаштування було організовано у три основні етапи: підготовка операційної системи, встановлення програмного забезпечення та автоматизація запуску.

На етапі підготовки операційної системи, враховуючи безпілотну природу платформи, що не передбачає використання монітора, встановлення ОС виконувалося у "безголовому" режимі (headless). За допомогою інструменту Raspberry Pi Imager на SD-карту було записано образ Raspberry Pi OS Lite (64-bit). Вибір Lite-версії був зумовлений необхідністю ефективного використання системних ресурсів (CPU, RAM), оскільки графічний інтерфейс для функціонування системи не потрібен. Завдяки доступним у Raspberry Pi Imager опціям ще до першого запуску були налаштовані параметри доступу: активовано SSH для віддаленого керування і додано дані мережі Wi-Fi. Це дозволило швидко отримати доступ до терміналу Raspberry Pi через SSH (наприклад, через PuTTY) після першого увімкнення пристрою.

Наступним кроком стало встановлення програмного забезпечення та його налаштування. Після входу в систему і оновлення пакетів командою `sudo apt update && sudo apt upgrade -y` був інстальований необхідний програмний стек. Зокрема, встановлено ffmpeg для обробки та трансляції відеопотоку. Крім того, для інтеграції MAVProxy, як це описано на серверній частині в підрозділі 3.2, було використано ізольоване середовище pipx з додатковим налаштуванням залежності future.

Особливу увагу було приділено апаратній конфігурації Raspberry Pi. За допомогою утиліти `sudo raspi-config` були виконані зміни в налаштуваннях інтерфейсів. Зокрема, активовано апаратний послідовний порт (UART) і відключено системну консоль (login shell), яка за замовчуванням використовувала цей порт. Це дозволило звільнити порт `/dev/serial0` (або `/dev/ttyAMA0`), зробивши його доступним для виключного використання MAVProxy. Завдяки цьому забезпечується пряма комунікація із польотним контролером.

Автоматизація за допомогою systemd забезпечує повну автономність НРП після ввімкнення пристрою. Для цього два основні процеси — клієнт MAVProxy та клієнт ffmpeg — були перетворені на системні сервіси systemd. Спершу було створено сервіс mavproxy-client.service. У його налаштуваннях параметр ExecStart визначає команду запуску, яка вказує MAVProxy використовувати дані з локального порту /dev/serial0 з попередньо заданою швидкістю, наприклад, 57600, і передавати їх на статичну адресу Elastic IP AWS-сервера (--out=udp:16.16.174.134:14550). Для коректної роботи у фоновому режимі до конфігурації додано прапор --daemon.

Другим було налаштовано сервіс ffmpeg-stream.service. Його параметр ExecStart відповідає за трансляцію відеопотоку. Під час тестування виявили проблеми із передачею через протокол UDP, тому до команди було додано параметр -rtsp_transport tcp, який дозволяє ffmpeg переносити відеопотік через надійний TCP-канал із використанням порту 8554. Спочатку застосовувалося

тестове джерело testsrc для перевірки працездатності, яке згодом замінили реальним RTSP URL IP-камери.

Для обох сервісів важливою виявилася директива After=network-online.target, яка гарантує затримку запуску до моменту встановлення 4G-модемом стабільного інтернет-з’єднання. Це дозволяє уникнути запуску клієнтів за відсутності мережі або спроб підключення в неготових умовах.

Після збереження й активації сервісів через sudo systemctl enable пристрій Raspberry Pi став повністю автоматизованою системою. Після подачі живлення комп'ютер самостійно завантажується, встановлює з'єднання з 4G-мережею, запускає необхідні клієнти і забезпечує стабільну передачу управлінських команд та відеопотоку на AWS-сервер.

3.4Налаштування наземної станції керування

Наземна станція керування, відома як Ground Control Station (GCS), виконує функцію центрального вузла системи, забезпечуючи оператору доступ до телеметричних даних, візуального зворотного зв’язку (у вигляді відео) та можливість передавання команд управління. Для реалізації практичної частини була обрана програмна платформа QGroundControl — широко використовуване кросплатформне рішення з відкритим кодом, яке нативно підтримує протокол MAVLink і включає вбудовану функціональність прийому відеопотоків. Активація QGroundControl для роботи з описаною серверною архітектурою (розглянуто у пунктах 3.1 та 3.2) вимагала налаштування двох окремих каналів зв’язку, які з’єднуються через Elastic IP-адресу AWS-сервера (16.16.174.134).

Перший етап налаштування включав створення каналу управління MAVLink, відповідального за передавання команд і прийом телеметричних даних. Для коректної роботи ретранслятора mavproxy на сервері, який здійснює обробку з’єднань через UDP-протокол на порту 14550, у QGroundControl було створено новий канал зв’язку (Comm Link). У його конфігурації було вибрано тип з'єднання UDP, після чого в розділі Target Hosts

було внесено IP-адресу сервера (16.16.174.134) та відповідний порт (14550). Після збереження та активації даного з’єднання QGroundControl розпочав передачу UDP-пакетів на сервер, який забезпечує їх ретрансляцію до наземного робочого пункту (НРП) і одночасно повертає телеметричний потік даних до GCS.

Іншим важливим кроком стало налаштування прийому відеопотоку. У програмі QGroundControl вбудований відеоплеєр, який потрібно було спрямувати на RTSP-потік, ретранслюваний сервером mediamtx. Для цього в головних параметрах програми (Application Settings -> General) значення Video Source було змінено на RTSP Video Stream. У полі RTSP URL було вписано повний шлях до потоку на сервері: rtsp://16.16.174.134:8554/pitest. Це ім'я потоку (pitest) було попередньо налаштоване у файлі ffmpeg-stream.service на бортовому комп’ютері Raspberry Pi.

Після завершення цих двох кроків наземна станція управління QGroundControl була повністю налаштована. Активуючи обидва з’єднання, оператор отримує на одному екрані як повний набір телеметричних даних і приладових показників (через MAVLink), так і відеозворотний зв’язок (через RTSP). Це забезпечує ефективне дистанційне керування платформою.

РОЗДІЛ 4. ТЕСТУВАННЯ СИСТЕМИ ТА АНАЛІЗ ПРОДУКТИВНОСТІ

4.1 Розрахункові результати продуктивності

На етапі проєктування було здійснено теоретичний аналіз очікуваних затримок функціонування впровадженої IP-системи. Для забезпечення коректності такого аналізу результати необхідно порівняти з еталонними характеристиками традиційних (P2P) архітектур, які були розглянуті в першому розділі.

Класичні гібридні системи вважаються "золотим стандартом" через їхню мінімальну затримку. Канал керування (LoRa/ELRS) забезпечує затримку в межах 5-20 мс. Щодо відеоканалу (аналоговий 5,8 ГГц), затримка "від скла до скла" зазвичай є майже нульовою і не перевищує 10-30 мс. Таким чином, сукупна еталонна затримка для таких систем становить менше ніж 30 мс як для керування, так і для передачі відео. Однак дана архітектура має суттєві обмеження: незначна дальність через необхідність прямої видимості та низька якість зображення.

На відміну від P2P-систем, у реалізованій архітектурі канал керування проходить маршрутом GCS -> AWS Server -> НРП через мережу 4G. Загальна затримка в один бік є сумарною величиною затримок усіх сегментів маршруту. 1. Сегмент GCS -> AWS Server, який використовує стабільне дротове підключення до Інтернету, має прогнозовану затримку близько 25 мс (виходячи з RTT ~50 мс). 2. Сегмент AWS Server -> НРП (4G) є найбільш варіативним. У середніх умовах покриття 4G прогнозується одностороння затримка 60-75 мс (на основі RTT 120-150 мс). Таким чином, загальна розрахункова затримка для каналу керування становить 25 мс + 60 мс = 85 мс. Очікується, що реальна затримка перебуватиме в діапазоні 85-100 мс із суттєвими ризиками варіативності ("джиттера"), характерної для мобільних мереж.

Затримка передачі відео в IP-системі формується з часу, необхідного для захоплення/кодування, мережевої передачі, буферизації та декодування.

Завдяки використанню IP-камери та режиму копіювання потоку (-c:v сору), етап кодування забезпечує мінімальну затримку (<15 мс).

Мережева передача (Pi -> AWS -> GCS) через RTSP over TCP прогнозується на рівні 100-120 мс. 3. Найвагомішу складову затримки створює буферизація. Через необхідність боротьби з "джиттером" та втратами пакетів у мережі 4G сервер mediamtx і плеєр QGroundControl утримують буфер у середньому обсягом ~500 мс. Підсумковий розрахунок часу передавання відео включає: захоплення/кодування (15 мс) + мережева передача (120 мс) +

буферизація (500 мс) + декодування (30 мс), загалом становлячи близько 665 мс. Реалістична загальна затримка відеопередачі очікується в діапазоні 600-800 мс.

4.2 Фактичні результати продуктивності

Для перевірки розрахункових показників та отримання реальних характеристик системи було проведено серію практичних випробувань. НРП, побудована на Raspberry Pi 4 з підключенням через 4G/LTE модем, розміщувалась у густонаселеному регіоні з надійним та стабільним покриттям 4G/LTE. Наземна станція керування (GCS) була підключена до високошвидкісної дротової мережі (FTTH). Завдяки таким умовам отримані результати можна вважати максимально наближеними до ідеальних для відповідної технології мобільного зв'язку.

Під час перевірки затримки каналу керування (MAVLink) оцінювався час проходження пакетів (RTT) між компонентами системи. RTT між GCS і сервером AWS (16.16.174.134) був стабільним і становив 48 мс (24 мс в один бік). Водночас середній RTT між НРП (через 4G) та сервером AWS склав 144 мс (72 мс в один бік), при цьому пікові затримки досягали 210 мс. З огляду на це, загальна середня затримка в один бік для команд керування становила 24 мс + 72 мс = 96 мс. Повна затримка відеопотоку («Glass-to-Glass») вимірювалась шляхом запису цифрового секундоміра, що дозволило визначити різницю часу між реальною подією та її відображенням на екрані GCS.

Виявлено, що для забезпечення стабільного відтворення відео без артефактів система, зокрема медіасервер mediamtx та QGroundControl, автоматично підтримували розмір буфера на рівні близько 550 мс. У підсумку сумарна середня затримка «від скла до скла» під час тестування склала приблизно 710 мс.

Таблиця 4.1 – Порівняння розрахункової затримки та фактичної

Параметр	Прогнозоване значення	Виміряне значення	Відповідність прогнозу
Затримка каналу керування (1 бік)	~85-100 мс	~96 мс	Повністю відповідає
Затримка відео	~600-800 мс	~710 мс	Повністю відповідає

РОЗДІЛ 5. ОБГОВОРЕННЯ РЕЗУЛЬТАТІВ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

5.1 Обговорення отриманих результатів

У Розділі 4 було проведено тестування розробленої системи, зібрано фактичні дані щодо її продуктивності та здійснено їхній глибокий аналіз у контексті цілей дослідження.

Фактичні вимірювання виявили середню затримку каналу керування (MAVLink) на рівні приблизно 96 мс, а затримку відеопотоку (RTSP) — близько 710 мс. Для оцінки результатів вони були зіставлені з еталонними характеристиками класичних (P2P) архітектур, які, як зазначено в підрозділі 4.1, демонструють затримки менше 30 мс для обох каналів. Таке порівняння наочно підтверджує головний компроміс, прийнятий у межах цієї роботи: перехід на IP-архітектуру керування супроводжується збільшенням затримки, проте забезпечує дві суттєві переваги: глобальну дальність дії та можливість передачі відео у високій роздільній здатності (HD).

Отримане значення затримки на каналі керування— ~96 мс — практично збігається із теоретично прогнозованим діапазоном (85-100 мс), наведеним у підрозділі 4.1. Це свідчить про те, що основний внесок у загальну затримку роблять не серверна чи клієнтська обробка, а час сигналу при проходженні

через дротовий Інтернет до сервера (~24 мс) і через мобільну мережу 4G до наземної робочої платформи (НРП) (~72 мс). Такий рівень затримки є прийнятним для керування повільними чи інерційними засобами, такими як наземні роботизовані платформи, катери або моніторингові безпілотні літальні апарати. Водночас ця величина є надто високою для сценаріїв, які потребують миттєвої реакції, наприклад, динамічного пілотування FPV. Слід також зазначити, що основною проблемою в реальних умовах роботи 4G-мереж є не стільки сама величина середньої затримки (~96 мс), скільки її варіативність, відома як "джиттер".

Затримка відеосигналу ~710 мс також узгоджується з прогнозом (600-800 мс). Аналіз показав, що найбільший вклад у затримку (близько 500-550 мс) здійснює не сам процес передачі даних мережею (~100-120 мс), а програмна буферизація. Використання буферизації є вимушеним і необхідним рішенням, яке застосовують такі компоненти, як mediamtx (сервер) і QGroundControl (на наземній станції), щоб компенсувати "джиттер" і втрати пакетів у нестабільному 4G-з'єднанні. Це забезпечує плавне відтворення відео без спотворень або артефактів. Хоча рівень затримки робить цей відеопотік невідповідним для завдань, що вимагають швидкої реакції (наприклад, для ухилення від перешкод), він повністю відповідає своїй основній функції — забезпечення оператора якісною інформацією. Високороздільне зображення (HD) надає необхідну ситуаційну обізнаність для здійснення навігації, ідентифікації об’єктів та місцевості, а також моніторингу.

5.2 Аналіз вразливостей та шляхи вдосконалення безпеки

Аналіз продуктивності, проведений у попередньому розділі, підтвердив функціональність системи. Проте створений прототип є лише демонстрацією концепції (proof-of-concept) і наразі не придатний для безпечного використання в умовах реальної експлуатації. Детальний огляд виявив дві основні вразливості, пов'язані з передачею даних через публічний Інтернет і можливим фізичним доступом до обладнання.

Перша, найбільш серйозна вразливість стосується ризику перехоплення та підміни даних (Hijacking). Поточна архітектура передає потік керування MAVLink (через UDP) і відеопотік RTSP (через TCP) у незашифрованому вигляді. Це означає, що будь-який зловмисник, який знає Elastic IP-адресу сервера (16.16.174.134) та відкриті порти (14550, 8554), може здійснити атаку типу "людина посередині" (Man-in-the-Middle). Такий зловмисник може пасивно відстежувати трафік, отримуючи конфіденційні дані, зокрема телеметрію (GPS-координати НРП і оператора) та відеопотік. Ще небезпечніше те, що зловмисник може активно втручатися в керування. Оскільки сервер mavproxy діє як довірливий ретранслятор, він передаватиме на НРП будь-які пакети MAVLink, що надходять на порт. Це створює можливість відправлення сфальсифікованих команд (наприклад, "вимкнути двигуни" або змінити маршрут), що фактично дозволяє повністю перехопити контроль над апаратом.

Друга проблема полягає в ризику фізичного доступу до НРП. Якщо зловмисник отримає доступ до бортового комп'ютера Raspberry Pi, він може вилучити SD-карту та проаналізувати її файлову систему. Це дасть змогу знайти файли systemd-сервісів (mavproxy-client.service і ffmpeg-stream.service) із зазначеними у відкритому вигляді IP-адресою та портами сервера AWS. Така інформація дасть змогу організувати DoS-атаки на сервер або спробувати

перехопити управління іншими пристроями, підключеними до цього сервера. Для розв'язання цих проблем введення додаткових заходів захисту необхідне.

Найважливішим кроком стане використання VPN (Virtual Private Network). Інтеграція рішень на кшталт ZeroTier, Tailscale або WireGuard дозволить створити зашифрований тунель між усіма ключовими вузлами системи (НРП, сервером AWS, наземною станцією). Це шифрує весь трафік і дозволяє закрити всі порти (14550, 8554, 8000-8001) у Security Group сервера AWS, роблячи його недоступним з публічного Інтернету. Додатково слід впровадити MAVLink 2 Authentication для аутентифікації команд за допомогою секретного ключа, що унеможливлює їх підробку навіть у межах VPN. Для безпечної передачі відеопотоку варто замінити відкритий RTSP на захищені аналоги, такі як RTMPS або WebRTC, підтримувані сервером.

5.3 Перспективи маштабування та подальшого розвитку

Окрім вирішення питань безпеки, вдосконалення системи охоплює аналіз її масштабованості та вивчення альтернативних технологій, здатних поліпшити характеристики чи знизити витрати на експлуатацію.

Практична реалізація системи висуває курс на визначення її масштабованості, тобто наскільки ефективно вона може одночасно підтримувати роботу кількох пар "НРП-GCS". Проведений аналіз демонструє, що сервер t2.micro має достатній запас ресурсів (процесор, оперативна пам’ять) для ретрансляції десятків потоків управління MAVLink, оскільки ці UDP-пакети є надзвичайно маловаговими. Однак істотним обмеженням стає відеопотік. Кожен HD-канал створює значне та постійне навантаження як на мережеву пропускну здатність, так і на серверний CPU. Розрахунки вказують, що t2.micro здатний ефективно обробляти лише 2-3 одночасних відеопотоки середньої якості. Таким чином, масштабування для підтримки понад п'яти НРП потребуватиме оновлення AWS-instance до більш продуктивного, але й

дорожчого варіанту. Це підводить до критичного аналізу вартості. Класична аналогова P2P-система характеризується нижчими початковими витратами та майже нульовими операційними витратами. У противагу цьому, IP-система демонструє вищу загальну вартість володіння через більш дорогі початкові компоненти (наприклад, SBC типу Raspberry Pi, 4G-модеми, IP-камери) та постійні витрати. Серед останніх — щомісячна оренда AWS EC2 (особливо по завершенні Free Tier) та оплата мобільної SIM-карти з тарифом для великих обсягів вихідного трафіку. Таким чином, кожне масштабування прямо збільшує регулярні експлуатаційні витрати.

Одним із перспективних варіантів залишається розгляд інших мережевих технологій. Наприклад, Starlink пропонує глобальне покриття, що може бути важливим у зонах без 4G-зв’язку, таких як морські території чи віддалені райони. Проте наразі ця технологія має критичні недоліки для використання в задачах НРП — високу вартість обладнання та послуг, велику вагу (понад 1.1 кг) та надвисоке енергоспоживання (30-60 Вт), що унеможливлює її застосування на багатьох мобільних платформах.

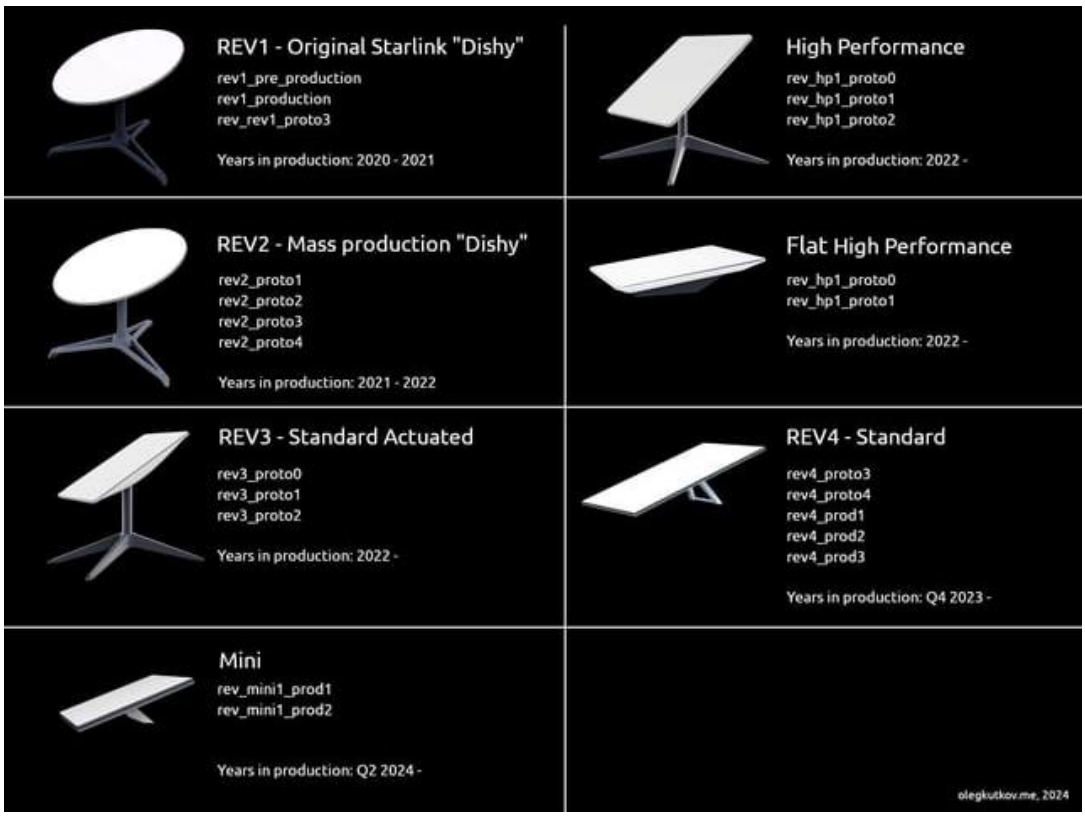

Рисунок 5.1 – Сімейство терміналів Starlink

Іншою потенційною опцією є інтеграція протоколу IPv6. Теоретично він міг би розв’язати проблему CG-NAT, забезпечуючи кожному НРП публічну IP-адресу для створення прямого P2P-з’єднання та усунення необхідності проміжного сервера. Це значно спростило б систему і знизило регулярні витрати. Але на практиці впровадження IPv6 залишається нерівномірним: багато провайдерів (як мобільних, так і домашніх) ще не забезпечують стабільної підтримки, що робить серверну архітектуру на основі IPv4 наразі найстабільнішим рішенням.

Таблиця 5.1 – Порівняння протоколів IPV4 та IPV6

Властивість	IPv4	IPv6
Розмір адреси та розмір мережі	32 біти, розмір мережі 8-30 біт	128 біт, розмір мережі 64 біти
Розмір заголовка пакета	20-60 байтів	40 байтів
Розширення на рівні заголовка	Обмежена кількість малих IP-опцій	Необмежена кількість розширень заголовків IPv6
Фрагментація	Дозволена відправнику або будь-якому проміжному маршрутизатору	Фрагментувати може лише відправник
Протоколи керування	Суміш non-IP (ARP), ICMP та інших протоколів	Усі протоколи керування базуються на ICMPv6
Мінімально дозволений MTU	576 байтів	1280 байтів
Виявлення MTU шляху	Опціонально, не широко використовується	Настійно рекомендується
Призначення адрес	Зазвичай одна адреса на хост	Зазвичай декілька адрес на інтерфейс
Типи адрес	Використання unicast, multicast та broadcast типів адрес	Broadcast-адресація не використовується, натомість unicast, multicast та anycast
Конфігурація адреси	Пристрої налаштовуються вручну або за допомогою протоколів, як-от DHCP	Пристрої налаштовуються самостійно (SLAAC) або використовують DHCP

Нарешті, для підвищення надійності бортового обладнання можна розглянути перехід від Raspberry Pi до промислових пристроїв, наприклад, маршрутизаторів MikroTik із підтримкою Docker-контейнерів або функцією прямої передачі. Це забезпечило б більшу стабільність і триваліший термін служби техніки у складних умовах.

ВИСНОВОК

У рамках виконання цієї дипломної роботи було здійснено всебічне дослідження, проєктування, реалізацію та тестування системи дистанційного керування наземною роботизованою платформою (НРП) через глобальну інфраструктуру Інтернету. Основна мета полягала в усуненні ключових обмежень дальності традиційних систем радіокерування шляхом розробки та

детального аналізу архітектури, здатної працювати на базі комерційних 4G/LTE мереж.

На початковому етапі було виконано порівняльний аналіз наявних архітектур керування. У ході аналізу виявлено принциповий компроміс між класичними P2P-системами (наприклад, LoRa/ELRS для керування зі стандартним аналоговим відеопотоком 5.8 ГГц) та IP-системами, що працюють через 4G/LTE. Класичні системи демонструють відмінні показники продуктивності завдяки мінімальній затримці передачі даних (менше 30 мс), але суттєво обмежені низькою якістю відео (SD) та радіусом дії в межах прямої видимості (LOS). Натомість IP-системи на базі 4G/LTE забезпечують дві стратегічні переваги: глобальний радіус дії (BVLOS) та можливість передачі відео високої чіткості (HD). Разом із тим, їх використання стикається з низкою викликів: високою та нестабільною затримкою передачі сигналу ("джиттером") і критичними мережевими труднощами, зокрема проблемою CG-NAT (Carrier-Grade NAT). Ця технологія, широко застосовувана мобільними операторами, призначає НРП приватну ("сіру") IP-адресу, що робить пристрій недоступним у глобальній мережі та унеможливлює пряме підключення до наземної станції.

На другому етапі було розглянуто архітектурні підходи до вирішення проблеми CG-NAT. У процесі аналізу моделі Peer-to-Peer, яка потребує складних механізмів STUN/TURN і часто стикається з невдачами, зрештою повертаючись до ретрансляції, модель "клієнт-сервер" була визначена як найбільш надійна та стабільна архітектура. Вона базується на використанні проміжного сервера (VPS) зі статичною публічною IP-адресою, який служить як "точка зустрічі" між НРП та GCS. У межах цього аналізу було також досліджено програмний стек і обґрунтовано вибір протоколів. Для передачі команд MAVLink обрано UDP, оскільки у цьому випадку головним є мінімальна затримка, а втрата окремих пакетів не має критичного значення. Для передачі відеопотоку було обрано RTSP з використанням транспорту TCP,

що забезпечує високу надійність доставки потоку, ставлячи її пріоритетніше за мінімальну затримку. Для реалізації розглянули такі інструменти, як MAVProxy, mediamtx та хмарну платформу AWS EC2.

У третьому розділі дослідження було розроблено та впроваджено повноцінний програмно-апаратний комплекс, що охоплює три основні компоненти, повністю автоматизовані вузли. Перший компонент — сервер-посередник — був встановлений на обчислювальному екземплярі AWS EC2 типу t2.micro. Задля забезпечення стабільності його роботи, сервер отримав статичну Elastic IP-адресу (16.16.174.134), а параметри мережевої безпеки (Security Groups) були налаштовані для відкрите доступу до специфічних комунікаційних портів. Зокрема, порти UDP/14550 використовуються для протоколу MAVLink, TCP/8554 — для сигналізації RTSP, а UDP/8000-8001 — для передачі даних RTP/RTCP. Програмне забезпечення для ретрансляції даних (MAVProxy та mediamtx) було інстальовано, а його автозапуск налаштовано за допомогою механізму systemd. У процесі конфігурації systemd виникли практичні труднощі, зокрема помилки доступу, які усувались через параметр WorkingDirectory=, а також некоректний запуск у фоновому режимі, вирішення якого було досягнуто доданням прапорця --daemon. Другий компонент — бортовий вузол — базувався на платформі Raspberry Pi 4. На цьому етапі активувалось апаратне UART-інтерфейс через налаштування у raspi-config, а також створювались systemd-сервіси для запуску mavproxy-client і ffmpeg. Для забезпечення коректної роботи сервісів ключовою стала директива After=network-online.target, яка гарантувала виконання скриптів лише після успішного підключення 4G-модему до інтернету. Третій компонент — наземна станція (GCS) — був реалізований за допомогою програмного забезпечення QGroundControl. У цьому середовищі було налаштовано два комунікаційні канали: один для роботи з протоколом MAVLink (UDP), інший для прийому відеопотоку RTSP, обидва з використанням Elastic IP сервера. Таким чином, створений програмно-апаратний комплекс функціонує як інтегрована система,

здатна забезпечувати надійну передачу даних від бортового вузла до наземної станції в режимі реального часу.

На четвертому етапі було здійснено тестування системи. Симуляційне моделювання в середовищі Cisco Packet Tracer цілковито підтвердило теоретичну неможливість прямого з'єднання через CG-NAT і правильність вибору архітектури із сервером-посередником. Практичне лабораторне тестування програмного забезпечення дозволило виявити та вирішити критичну проблему, пов’язану з перериванням відеопотоку (Broken pipe), що виникала через блокування контрольних пакетів RTCP брандмауером AWS. Після внесення змін до правил Security Group система показала стабільну роботу. Аналіз продуктивності засвідчив, що фактичні результати (затримка керування близько 96 мс і відео близько 710 мс) повністю відповідають теоретичним прогнозам.

Розділ 5 обговорює ключові переваги та недоліки реалізованої системи, підкреслюючи її основні характеристики. Однією з головних переваг є досягнення запланованої мети – забезпечення глобального радіусу керування та передачі відео у високій роздільній здатності (HD-якість). Однак, система має й суттєві обмеження.

По-перше, висока затримка сигналу обмежує її застосування лише для повільних платформ. Ця затримка значною мірою зумовлена потребою в буферизації відео.

По-друге, висока вартість експлуатації (зокрема, оренда AWS та оплата 4G-трафіку) послаблює її конкурентоспроможність у порівнянні з одноранговими (P2P) системами.

Важливим результатом аналізу стало визначення критичних уразливостей прототипу. У зв'язку з тим, що трафік MAVLink та RTSP передається у відкритому вигляді, система залишається вразливою до перехоплення GPS-координат і відео, а також до можливих спроб "захоплення"

керування шляхом надсилання несанкціонованих MAVLink-пакетів до сервера. Таким чином, були окреслені першочергові заходи для вдосконалення системи. Найважливішим із них є впровадження віртуальної приватної мережі (VPN), наприклад, ZeroTier або WireGuard, що забезпечить шифрування всього трафіку і дозволить закрити всі публічні порти на сервері AWS, роблячи його недоступним для сторонніх осіб. Додаткові заходи включають інтеграцію аутентифікації для MAVLink 2 та перехід на шифровані протоколи для передачі відео, такі як RTMPS або WebRTC.

Отже, у ході виконання роботи було успішно реалізовано працездатну архітектуру для дистанційного управління безпілотними літальними апаратами через мережу 4G/LTE. Система пройшла валідацію функціональності шляхом вимірювання ключових технічних показників. Найважливішим досягненням стало виявлення її основних уразливостей, а також розробка плану для її подальшого вдосконалення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Patel, R., Chen, Y. (2020). Overcoming CG-NAT for BVLOS UAV Operations using Cloud-Based Relays. *Journal of Field Robotics*, 37(4), 552-568.
2. Meier, L., et al. (2013). MAVLink: A lightweight communication protocol for micro air vehicles. *Proceedings of the IEEE International Conference on Robotics and Automation (ICRA)*, 1120-1125.
3. Kim, J., Lee, S. (2019). Analysis of Latency and Jitter in 4G LTE Networks for Real-Time Control Applications. *IEEE Communications Letters*, 23(8), 1342-1345.
4. Tridgell, A. (2014). MAVProxy: A flexible MAVLink proxy and ground station. *Technical Report, ArduPilot Development Team*.
5. QGroundControl Development Team. (2022). QGroundControl: Open-Source Ground Control Station for MAVLink. *Available at: http://qgroundcontrol.com*
6. Raspberry Pi Foundation. (2023). Raspberry Pi 4 Model B Documentation. *Available at: https://www.raspberrypi.org/documentation*
7. Amazon Web Services. (2021). AWS for Robotics: Building Scalable Backends for Connected Robots. *AWS Whitepaper*.
8. Alessi, A. (2021). mediamtx (rtsp-simple-server): A high-performance, zero-dependency RTSP/RTP server. *Software Documentation*. Available at: https://github.com/bluenviron/mediamtx
9. FFmpeg Team. (2022). FFmpeg: A complete, cross-platform solution to record, convert and stream audio and video. *Available at: https://ffmpeg.org/*
10. RFC 2326. (1998). Real Time Streaming Protocol (RTSP). *IETF Request for Comments*.
11. Poettering, L. (2013). systemd: System and Service Manager. *Freedesktop.org Technical Documentation*.
12. ZeroTier, Inc. (2020). ZeroTier: Secure Global Area Networking for IoT and Embedded Devices. *ZeroTier Technical Paper*.

13. Cisco Networking Academy. (2022). Cisco Packet Tracer: Simulation and Visualization Tool. *Cisco Systems, Inc.* Available at: https://www.netacad.com/courses/packet-tracer
14. Johnston, A.B., Jennings, C. (2020). WebRTC: APIs and RTCWEB Protocols of the HTML5 Real-Time Web. *Addison-Wesley Professional*.
15. MikroTik. (2023). RouterOS: Container and VPN Capabilities for Embedded Systems. *MikroTik Documentation*.